WildPackets Academy

2540 Camino Diablo • Walnut Creek, CA 94596 • 925.937.7900 • fax 925.937.2479 • www.wildpacketsacademy.com

Janet shu

WildPackets Academy

phell shade

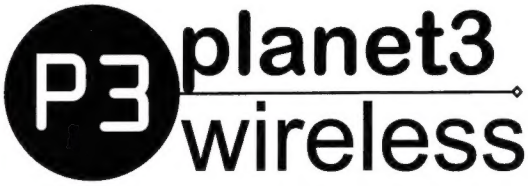
Wireless LAN Administration
WP-106 (CWNA)

Optimizing network education

WildPackets, Inc.
1340 Treat Blvd., Ste. 500
Walnut Creek, CA 94597
www.wildpackets.com
(925)937-3200 fax (925)937-3211

WildPackets Academy

working together with



is pleased to bring you this newly updated version of the WildPackets Academy WP-106 wireless network analysis training course.

WildPackets Academy, Planet3 Wireless, and the Wireless LAN Association

The Wireless LAN Association is a non-profit educational trade association, comprised of the thought leaders and technology innovators in the local area wireless technology industry. WLANA provides a clearinghouse of information about wireless local area applications, issues and trends and serves as a resource to customers and prospects of wireless local area products and to industry press and analysts. The Association maintains an educational web site at www.wlana.org.

In February, 2002, Planet3 Wireless, Inc. announced that the Wireless LAN Association (WLANA) officially endorsed the Certified Wireless Network Administrator (CWNA) certification. WLANA is the educational trade association for the wireless networking industry. The executive director of WLAN reviewed the curriculum and "found it to be a high quality offering, worthy of WLANA endorsement." He went on to say, "Through our Educational Endorsement Program, WLANA will continue to recognize vendor neutral programs, such as CWNA, that will increase the knowledge, skills, and competence of professionals in the wireless LAN industry."

The instructors and courseware developers at WildPackets Academy worked closely with the technical experts and content developers at Planet3 Wireless to make the CWNA curriculum available through WildPackets Academy and we're pleased to provide you, our students, with the coupling of the AiroPeek wireless protocol analyzer with the technical content of the CWNA certification program.

Whether you're attending this course as part of preparing for CWNA certification, or simply as a way of learning how to administer, troubleshoot, and analyze your 802.11 network using AiroPeek NX, you'll find the scope and depth of material, as well as the hands-on lab exercises, ideally suited to your needs.

Planet3 Wireless, Inc.
PO Box 412
Bremen GA 30110
866-GET-CWNE
www.cwne.com

The information provided in this manual is provided as-is and is subject to change without notice. All content in this manual are believed to be accurate but are presented without warranty of any kind, express or implied.

LICENSE
PLEASE READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS MANUAL ("MATERIALS"). BY USING THE MATERIALS YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS LICENSE.

NO PART OF THIS DOCUMENT MAY BE REPORDUCED OR TRANSMITTED IN ANY FORM OR BY ANY MEANS, ELECTRONIC OR MECHANICAL, FOR ANY PURPOSE, WITHOUT THE EXPRESS WRITTEN PERMISSION OF PLANET3 WIRELESS.

THE MATERIALS THEREIN ARE PROVIDED "AS IS". PLANET3 WIRELESS MAKES NO REPRESENTATIONS OR WARRANTIES, EITHER EXPRESS OR IMPLIED, OF ANY KIND WITH RESPECT TO THE MATERIALS, THEIR CONTENTS, OR INFORMATION. PLANET3 WIRELESS EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, OF ANY KIND WITH RESPECT TO THE MATERIALS OR THEIR USE, INCLUDING BUT NOT LIMITED TO MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. YOU AGREE THAT PLANET3 WIRELESS, ITS DIRECTORS, OFFICERS, EMPLOYEES OR OTHER REPRESENTATIVES SHALL NOT BE LIABLE FOR DAMAGES ARISING FROM THE CONTENT OR USE OF THE MATERIALS. YOU AGREE THAT THIS LIMITATION OF LIABILITY IS COMPREHENSIVE AND APPLIES TO ALL DAMAGES OF ANY KIND, INCLUDING WITHOUT LIMITATION DIRECT, INDIRECT, COMPENSATORY, SPECIAL, INCIDENTAL, PUNITIVE AND CONSEQUENTIAL DAMAGES.

CWNA, CWNI, CWNP, CWSP, CWNE are trademarks of Planet3 Wireless, Inc.

Other trademarks and manufacturer graphics referenced are the property of their respective owners.

Certified Wireless Network Administrator, Revision 1.8, Course Guide
Copyright © 2003 Planet3 Wireless, Inc.
All rights reserved. Printed in the USA.

Acknowledgements

This section acknowledges the efforts of those who contributed significantly to defining Certified Wireless Network Administrator course and making it successful.

Please send specific feedback on the CWNA program or this manual via email to *feedback@cwne.com*.

CWNA Core Curriculum Team

- Kevin Sandlin, kevin@p3wireless.com
- Scott Turner, scott@p3wireless.com
- Devin Akin, devin@p3wireless.com
- Jeff Jones
- Josh McCord
- Robert Nicholas
- Stan Brooks

Copyright © 2003, Planet3 Wireless, Inc.

Contents

Introduction	**Course Overview**	i
	Course Objectives	ii
	Prerequisites	iii
	Information Sources	iv
	Course Outline	v
Chapter 1	**Introduction to Wireless LANs**	**1-1**
	Objectives	1-1
	Chapter Content	1-2
	Wireless LAN Market Overview	1-3
	Applications of a Wireless LAN	1-5
	FCC	1-8
	IEEE	1-9
	WLIF	1-10
	The Wi-Fi Alliance	1-11
	WLANA	1-12
Chapter 2	**Radio Frequency Fundamentals**	**2-1**
	Objectives	2-1
	Chapter Content	2-2
	RF	2-3
	Voltage Standing Wave Radio	2-5
	Antennas	2-7
	RF Math	2-8
	RF Math Exercises	2-12
Chapter 3	**Spread Spectrum Technologies**	**3-1**
	Objectives	3-1
	Chapter Content	3-2
	Spread Spectrum	3-3
	Modulation	3-5

Copyright © 2003, Planet3 Wireless, Inc.

	Frequency Hopping Spread Spectrum	3-7
	Direct Sequencing Spread Spectrum	3-10
	FHSS vs. DSSS	3-12
	Throughput and Range	3-14
Chapter 4	**Wireless LAN Infrastructure Devices**	**4-1**
	Objectives	4-1
	Chapter Content	4-2
	Access Point	4-3
	Using Access Points	4-4
	Access Point in Root Mode	4-5
	Access Point in Repeater Mode	4-6
	Access Point in Bridge Mode	4-7
	Mounting	4-8
	Bridges	4-9
	Wireless Bridge	4-9
	Wireless Workgroup Bridges	4-11
	Client Devices	4-13
	PCMCIA Cards and Converters	4-14
	Wireless Adapters	4-15
	Gateways	4-18
	Wireless Residential Gateways	4-18
	Enterprise Wireless Gateway	4-21
Chapter 5	**Antennas and Accessories**	**5-1**
	Objectives	5-1
	Chapter Content	5-2
	RF Antennas	5-3
	Dipole/Omni-directional	5-3
	Semi-directional	5-7
	Highly-directional	5-10
	Grid	5-12
	Polarization	5-14
	Antenna Gain and Beamwidth	5-15
	Antenna Mounts	5-17
	Antenna Installation and Configuration	5-19
	Antenna Safety	5-21
	Power over Ethernet	5-23
	Wireless LAN Accessories	5-25
	RF Amplifiers	5-25
	RF Attenuators	5-28
	Lightning Arrestors	5-30

Copyright © 2003, Planet3 Wireless, Inc.

	RF Splitters	5-32
	RF Connectors	5-35
	RF Cables	5-37
	Pigtails	5-39
	Frequency Converter	5-40
	Bandwidth Control Units	5-42
	Test Kits	5-44
Chapter 6	**Wireless LAN Organizations and Standards**	**6-1**
	Objectives	6-1
	Chapter Content	6-2
	FCC Regulations	6-3
	ISM and UNII Spectra	6-4
	Radiated Power Consumption	6-6
	IEEE and 802.11	6-9
	Standards and Drafts	6-10
	HomeRF	6-13
	Bluetooth	6-15
	Infrared	6-16
	ETSI	6-18
Chapter 7	**802.11 Network Architecture**	**7-1**
	Objectives	7-1
	Chapter Content	7-2
	Authentication and Association	7-3
	Authentication Process Types	7-5
	Open System Authentication	7-5
	Shared Key Authentication	7-6
	Service Sets	7-7
	Basic Service Set	7-7
	Extended Service Set	7-8
	Independent Basic Service Set	7-9
	Beacons	7-10
	Power Management Modes	7-12
	Infrastructure Power Management	7-13
	Ad Hoc Power Management	7-14
	Dynamic Rate Shifting	7-16
Chapter 8	**MAC & Physical Layers**	**8-1**

Copyright © 2003, Planet3 Wireless, Inc.

	Objectives	8-1
	Chapter Content	8-2
	Communication Modes	8-3
	Joining a Network	8-3
	Interframe Spacing	8-5
	Collision Handling	8-7
	RTS/CTS	8-8
	RTS/CTS Handshaking	8-8
	RTS/CTS Process	8-10
	Fragmentation	8-11
Chapter 9	**Troubleshooting Wireless LAN Installations**	**9-1**
	Objectives	9-1
	Chapter Content	9-2
	Multipath	9-3
	Antenna Diversity	9-5
	Hidden Node	9-6
	Near/Far	9-8
	Co-location Throughput	9-10
	Channel Reuse	9-12
	Interference	9-13
Chapter 10	**Wireless LAN Security**	**10-1**
	Objectives	10-1
	Chapter Content	10-2
	Introduction to Wireless LAN Security	10-3
	Wired Equivalent Privacy	10-4
	Why WEP Was Chosen	10-6
	Implementing WEP Keys	10-7
	Using WEP	10-8
	Managing WEP Keys	10-10
	Advanced Encryption Standard	10-11
	Access Point and Bridge Security	10-12
	Service Set Identifier	10-13
	Using MAC Filters	10-14
	Eavesdropping	10-15

Copyright © 2003, Planet3 Wireless, Inc.

Wireless Packet Analyzers 10-16

How Attacks Occur 10-17
- Broadcast Monitoring 10-17
- Rogue Access Points 10-18
- Accessing Configuration Interfaces 10-18
- Man-in-the-Middle Attacks 10-19

Wireless Security Management 10-20

Corporate Security Policy 10-22

Security Recommendations 10-24
- Change Wireless LAN Authentication 10-24
- Choose Scalable Solutions 10-24
- Add Additional Security Services 10-25
- Schedule Access Point Discovery 10-25
- Schedule Security Audits 10-25
- Distributed Personal Firewalls or IDS Agents 10-25
- Monitor the Network 10-25
- Connect Access Points to Switches 10-25
- Implement a Wireless DMZ 10-26

Chapter 11 RF Site Survey Fundamentals 11-1

Objectives 11-1

Chapter Content 11-2

What Is A Site Survey? 11-3

Interviewing Network Managers 11-4
- The Purpose of the Wireless LAN 11-5
- Business Requirements 11-6
- Security Requirements 11-9
- Available Resources 11-11
- Existing Networks 11-13

Locating RF Interference 11-16
- Spectrum Analysis 11-16
- Locating Sources of RF 11-18
- Obstacle-Induced Signal Loss 11-20

Determining Contours of RF Coverage 11-21
- Obtaining Measurements 11-22
- Locating Zones 11-22
- Discovering Coverage Gaps 11-22
- Antenna Testing 11-23

Locating Hardware Installation Points 11-24

Towers 11-26

Lifts and Ladders 11-27

Documenting Installation Issues 11-28
- Indoor Installation Issues 11-28

Copyright © 2003, Planet3 Wireless, Inc.

Outdoor Installation Issues 11-29
Earth Bulge 11-29
Weather 11-30

Spot Checks 11-31

Reporting 11-32
Application and Requirements Analysis 11-32
Interference Source Analysis 11-33
RF Coverage Analysis 11-33
Hardware Placement and Configuration 11-33
Reporting Tips 11-34
Additional Reporting 11-35

Chapter 12 **Lab Exercises** **12-1**

Lab 1 – Infrastructure Mode Connectivity 12-2

Lab 2 – Infrastructure Mode Throughput Test 12-5

Lab 3 – Ad Hoc Connectivity & Throughput Tests 12-8

Lab 4 – Cell-sizing and Automatic Rate Selection (ARS) in Infrastructure Mode 12-11

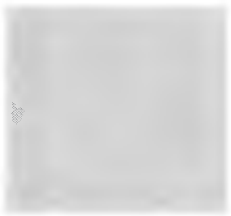
Lab 5 – Rudimentary Security Features with Seamless Roaming in an Extended Service Set 12-14

Lab 6 – Throughput in a Co-location Environment 12-17

Lab 7 - Dynamic WEP keys and mutual authentication using 802.1x/EAP and RADIUS 12-22

Lab 8 - Wireless VPN using PPTP tunnels and RADIUS 12-26

Copyright © 2003, Planet3 Wireless, Inc.

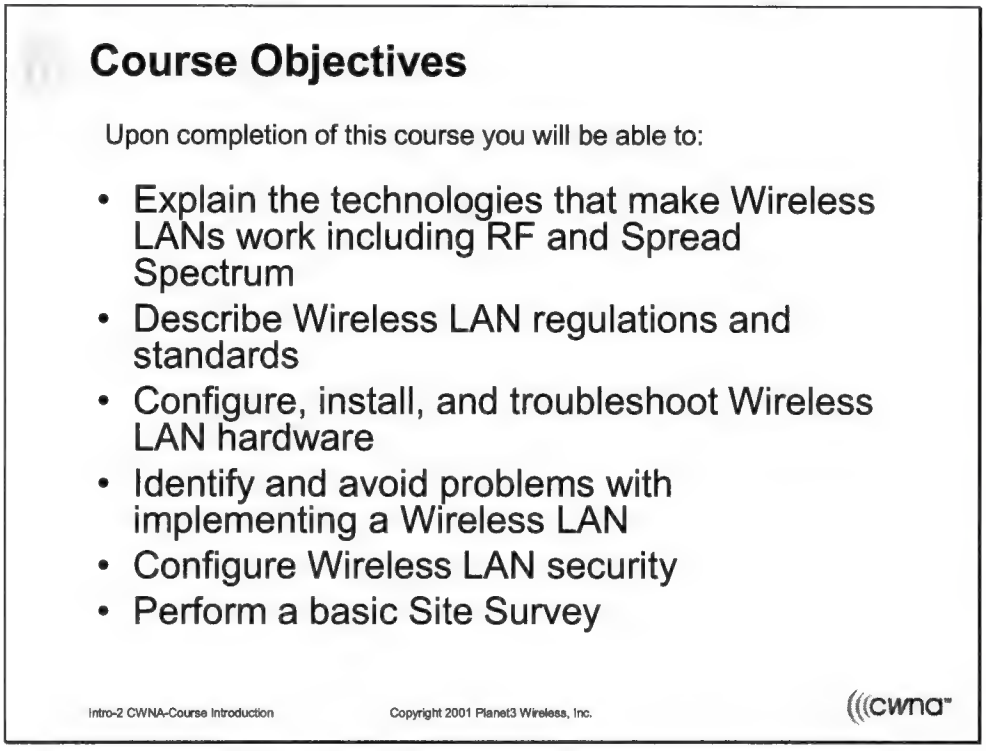


Introduction

Introduction

The Wireless LAN Administration course is an instructor-led course provided to students who want to learn a broad range of information about administering wireless LANs. This course focuses on the knowledge an IT professional needs to successfully install, configure, and maintain wireless LANs. The material covered in this course is vendor-neutral, in that it does not teach about one specific vendor's product line, but instead teaches wireless LAN technology. By learning vendor-neutral information, a student will be able to apply their knowledge to any vendor's product line.

Copyright © 2003, Planet3 Wireless, Inc.

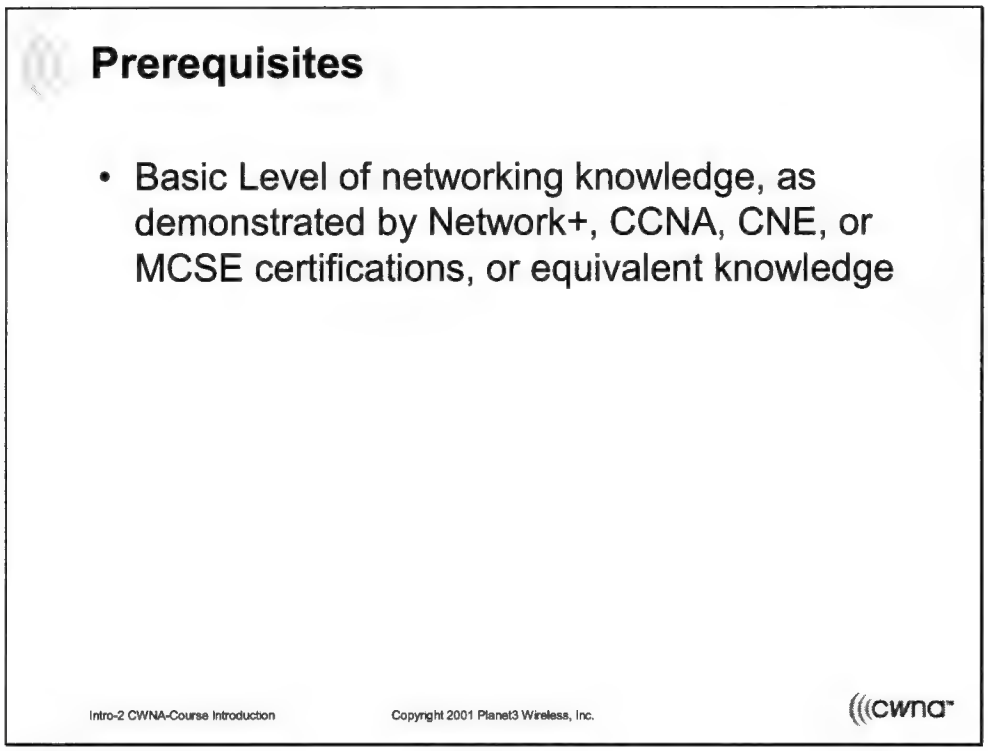

Course Objectives
Upon completion of this course you will be able to:
• Explain the technologies that make Wireless LANs work including RF and Spread Spectrum
• Describe Wireless LAN regulations and standards
• Configure, install, and troubleshoot Wireless LAN hardware
• Identify and avoid problems with implementing a Wireless LAN
• Configure Wireless LAN security
• Perform a basic Site Survey
Intro-2 CWNA-Course Introduction
Copyright 2001 Planet3 Wireless, Inc.
cwna

Course Objectives

Upon completion of this course, the student will be able to:

- Define and apply the basic concepts of Radio Frequency (RF) technology including spread spectrum technologies and how they apply to wireless LANs.
- Understand and explain the fundamental principles and concepts that are used in wireless LANs, allowing students to be better able to analyze and solve problems.
- Describe the organizations and laws that govern wireless LANs, so that students can comply with any regulations that may be involved with the setup and maintenance of a wireless LAN.
- Install, setup, and maintain a wireless network using the different hardware devices that will be introduced such as access points, bridges, gateways, and antennas.
- Analyze and troubleshoot the problems that can occur with wireless LAN data transmission, including multipath, hidden nodes, and interference.
- Perform a basic site survey for the installation of a wireless LAN, and explain what needs to be taken into consideration.
- Secure the transmission of data over a wireless LAN, and identify the different types of attacks that can occur from hackers.

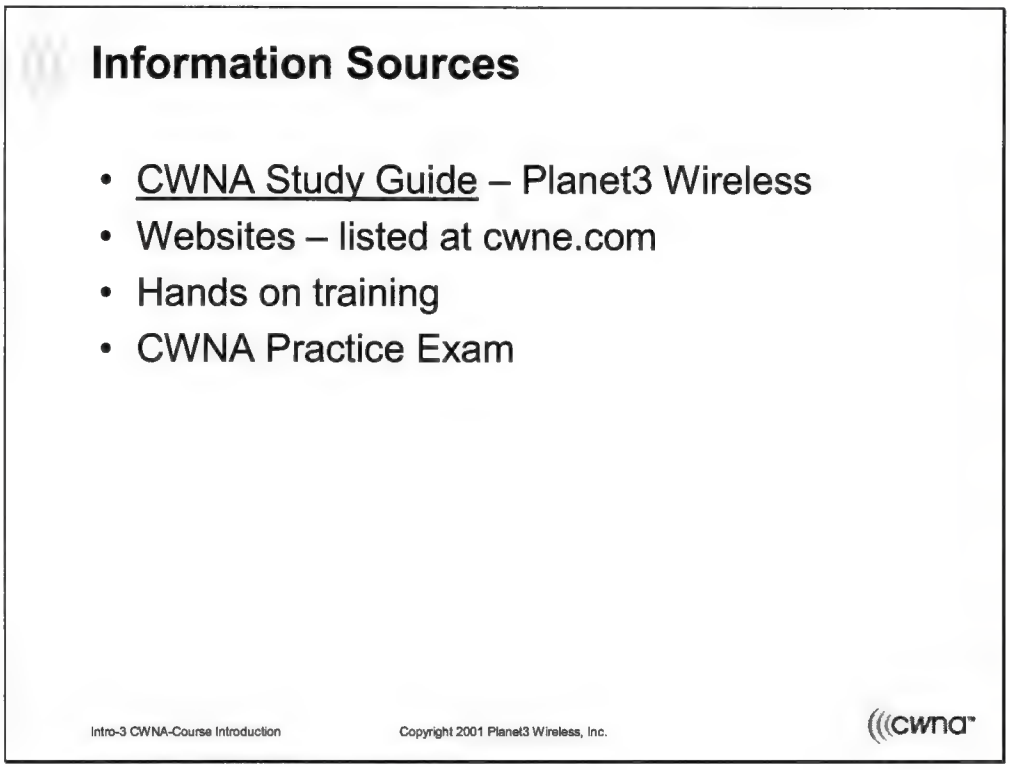
Copyright © 2003, Planet3 Wireless, Inc.


Prerequisites
• Basic Level of networking knowledge, as demonstrated by Network+, CCNA, CNE, or MCSE certifications, or equivalent knowledge
Intro-2 CWNA-Course Introduction
Copyright 2001 Planet3 Wireless, Inc.
cwna

Prerequisites

The Wireless LAN Administration course focuses on introducing wireless LAN technology and wireless networking concepts. To fully benefit from this course and the materials presented the student should have a level of networking knowledge similar to that provided by the Network+, CCNA, CNE, or MCSE certifications, or knowledge that is similar to that which is tested by these certifications.

Copyright © 2003, Planet3 Wireless, Inc.

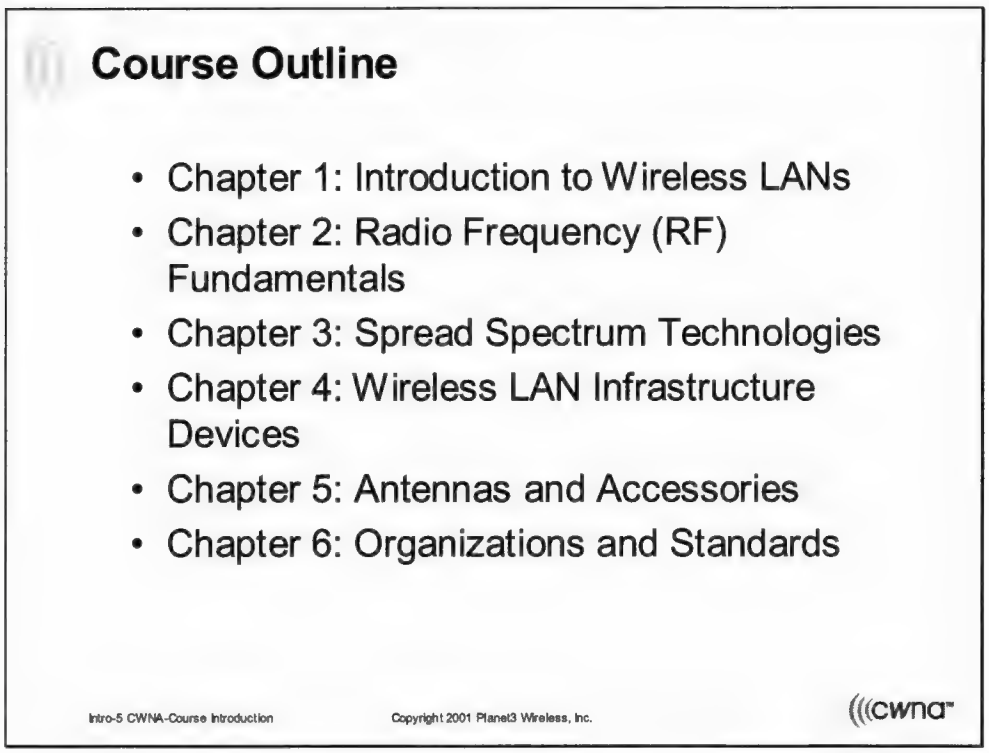

Information Sources
• CWNA Study Guide – Planet3 Wireless
• Websites – listed at cwne.com
• Hands on training
• CWNA Practice Exam
Intro-3 CWNA-Course Introduction
Copyright 2001 Planet3 Wireless, Inc.
cwna

Information Sources

After completion of the Wireless LAN Administration course, students may want to further their studies in preparing for the exam or to focus on one particular area of study, such as security or site surveys. The following list includes sources of information that are recommended to further a student's knowledge of wireless LANs:

- CWNA Study Guide. This book from Planet3 Wireless contains extensive information on the administration of wireless LANs, and prepares students to take the CWNA exam.
- Official CWNA Practice Test. This practice exam is available from cwne.com as a browser-based, online practice test. The practice test consists of over 300 test questions that are very similar to the questions that candidates will actually see on the CWNA certification exam.
- The Internet provides many websites that focus on wireless LANs and also provides whitepapers for specific areas of study. A list of websites that provide this type of information is available at http://www.cwne.com/cwnp/training_resources.html.
- Students should seek to obtain hands on experience where possible. The labs that are part of this course are hands on and teach students a great deal of information, but are limited to the duration of the course.

Copyright © 2003, Planet3 Wireless, Inc.


Course Outline
• Chapter 1: Introduction to Wireless LANs
• Chapter 2: Radio Frequency (RF) Fundamentals
• Chapter 3: Spread Spectrum Technologies
• Chapter 4: Wireless LAN Infrastructure Devices
• Chapter 5: Antennas and Accessories
• Chapter 6: Organizations and Standards
Intro-5 CWNA-Course Introduction
Copyright 2001 Planet3 Wireless, Inc.
cwna

Course Outline

Chapter 1, "Introduction to Wireless LANs", presents an overview of wireless LAN technology and explains where wireless networks should be applied. Regulation-making organizations, industry organizations, wireless LAN standards, and standards-making organizations are discussed. The major hardware vendors and which solutions each manufacturer offers to the marketplace are discussed.

Chapter 2, "Radio Frequency (RF) Fundamentals", explains the importance of RF technology and the role it plays in wireless communications. RF math is discussed to demonstrate how RF math is used to calculate signal strength, keep a wireless network within FCC regulations, and to assemble a secure, precise wireless network. The cause and application of basic RF antenna concepts are illustrated to show how radio waves and antennas interact. RF behavior and modulation types are discussed along with problems that could be encountered with improper wireless LAN configurations. Specific RF and wireless LAN technology terms are defined and concepts explained.

Chapter 3, "Spread Spectrum Technologies", explains why and how spread spectrum technology is used with wireless LANs. Regulations concerning wireless LANs and a comparison between the different types of spread spectrum technologies are discussed in detail.

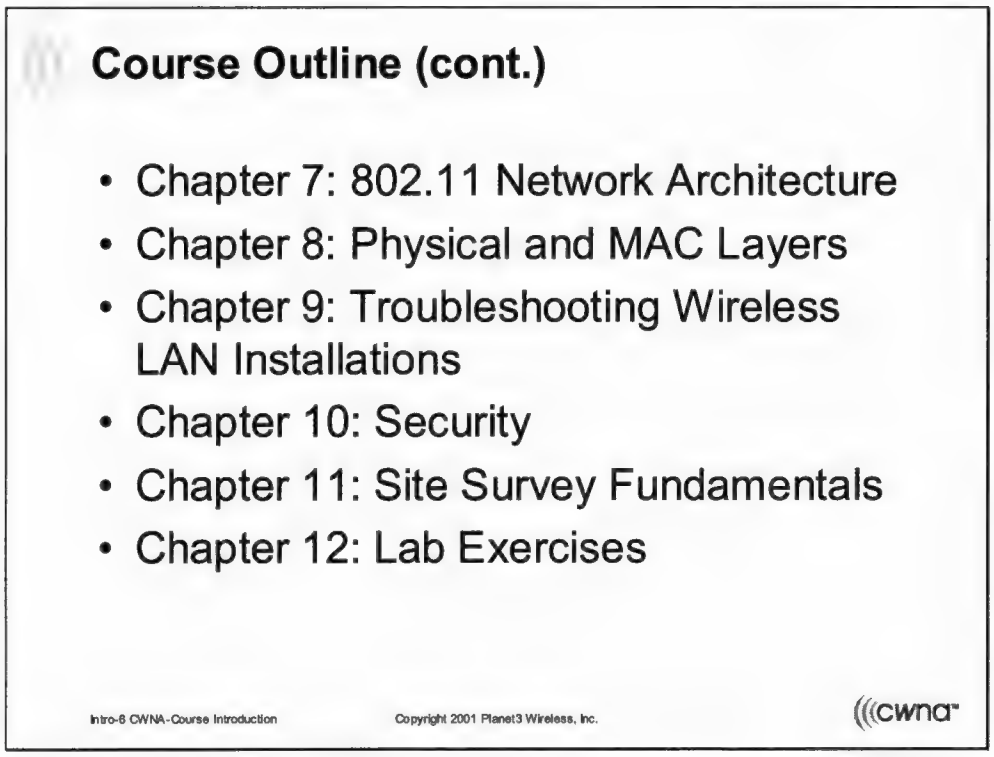
Copyright © 2003, Planet3 Wireless, Inc.

Chapter 4, "Infrastructure Devices", discusses the installation, configuration, and management of wireless LAN hardware devices, including client devices, enterprise devices, and connectivity of wired and wireless networks.

Chapter 5, "Antennas and Accessories", covers the specifications, types, and effects of wireless LAN accessories along with appropriate uses of them. Antenna types, uses, configurations, and characteristics will be covered in detail for both indoor and outdoor uses.

Chapter 6, "Organizations and Standards", focuses on regulations created by the FCC, the ISM & UNII bands and their role in wireless LANs, emerging wireless LAN technologies, and current IEEE standards and drafts. The FCC's and IEEE's roles in defining and using the ISM & UNII bands will be discussed at length. IEEE standards and how they fall within the FCC guidelines will be covered in detail.

Copyright © 2003, Planet3 Wireless, Inc.


Course Outline (cont.)
• Chapter 7: 802.11 Network Architecture
• Chapter 8: Physical and MAC Layers
• Chapter 9: Troubleshooting Wireless LAN Installations
• Chapter 10: Security
• Chapter 11: Site Survey Fundamentals
• Chapter 12: Lab Exercises
Intro-8 CWNA-Course Introduction
Copyright 2001 Planet3 Wireless, Inc.
cwna

Course Outline

Chapter 7, "802.11 Network Architecture", will describe authentication & association and their roles in wireless LAN connectivity. The various types of service sets and how they are used will be explained, and details of power management, both in Infrastructure and Ad Hoc modes, will be covered.

Chapter 8, "Physical and MAC Layers", presents an overview of both Layer 1 and Layer 2 functionality of wireless LANs. The modes of operation wireless LANs use for contention and polling are discussed. The CSMA/CA and RTS/CTS protocols are broken down into an understandable format, and both types of scanning are covered in detail. Interframe spacing and handling of collisions are among the topics covered in this section.

Chapter 9, "Troubleshooting Wireless LAN Installations", will cover common problems associated with wireless LANs. Multipath and its symptoms and affects will be discussed at length, along with the techniques and solutions used to compensate for it. Many types of common RF interference will be explained, and issues affecting outdoor links such as Earth bulge will be discussed. Maximizing throughput and avoiding co-channel and adjacent channel interference in co-location environments will be covered.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter 10, "Security", discusses methods of attacking wireless LANs, security measures specified by IEEE, common solutions implemented by manufacturers, and leading-edge products for protecting wireless LANs. Various implementation solutions are discussed, and WEP is covered in detail. Forthcoming security measures such as AES, 802.1x/EAP, and VPNs are also discussed. Common security faults, scalable security methodology, and examples of common security-related problems are presented.

Chapter 11, "Site Survey Fundamentals", provides information on how to specify what needs to be done prior to wireless LAN installations. Input from different wireless consulting companies and many different professionals is presented on how to best perform a site survey under given conditions. General information that is agreed upon across the industry as well as many different views of how to perform associated tasks is presented. Covered topics include determining the business needs for an organization that wishes to install a wireless LAN, locating appropriate installation locations for wireless LAN hardware, finding and avoiding RF interference, and creating an RF site survey report.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

1 Introduction to Wireless LANs

Objectives

Upon completion of this chapter you will be able to:

- Describe the wireless LAN Market and the standards that govern the market
- Describe the appropriate applications of a wireless LAN and how wireless LANs should best be used
- Define the major wireless LAN organizations and the role each organization plays

1-2 CWNA-Introduction to Wireless LANs Copyright 2002 Planet3 Wireless, Inc.

Chapter Content

Wireless LAN technology has many different applications in the enterprise, for small businesses, and even for homes. As the technology changes, new standards are introduced that have different features and benefits for these applications. The organizations that define and support these technologies play an important role in the marketplace.

Chapter 1 introduces the wireless LAN market and the different organizations that have an impact on the marketplace. The current 802.11 standards are introduced along with the organizations that define and support the standards. Applications in which wireless LANs can and should be used are also discussed.

The chapter outline is as follows:

- Wireless LAN Market Overview
- Applications of a Wireless LAN
- FCC
- IEEE
- The Wi-Fi Alliance
- WLIF
- WLANA

Copyright © 2003, Planet3 Wireless, Inc.

Wireless LAN Market Overview

- Past, Present, Future of wireless LANs
- Introduction to current standards
  - IEEE 802.11
  - IEEE 802.11b
  - IEEE 802.11a
  - IEEE 802.11g

1-3 CWNA-Introduction to Wireless LANs Copyright 2002 Planet3 Wireless, Inc. (((cwna

The Wireless LAN Market

Wireless networks were first used by the military as an easy and secure way to exchange information in the field of battle. Because the technology was cost prohibitive, corporate adoption took much longer. The first wireless technologies that became available in the marketplace were proprietary implementations. Thus, if an organization chose to use wireless technology, that organization was forced to use only a single vendor's solution for fear of incompatibilities with other vendors' hardware.

With the introduction of the 802.11 standard from the IEEE (The Institute of Electrical and Electronics Engineers, www.ieee.org), vendors had a common set of rules for developing wireless networking hardware. The issues of hardware compatibility were basically removed as long as organizations used hardware that was compliant with the IEEE 802.11 standard.

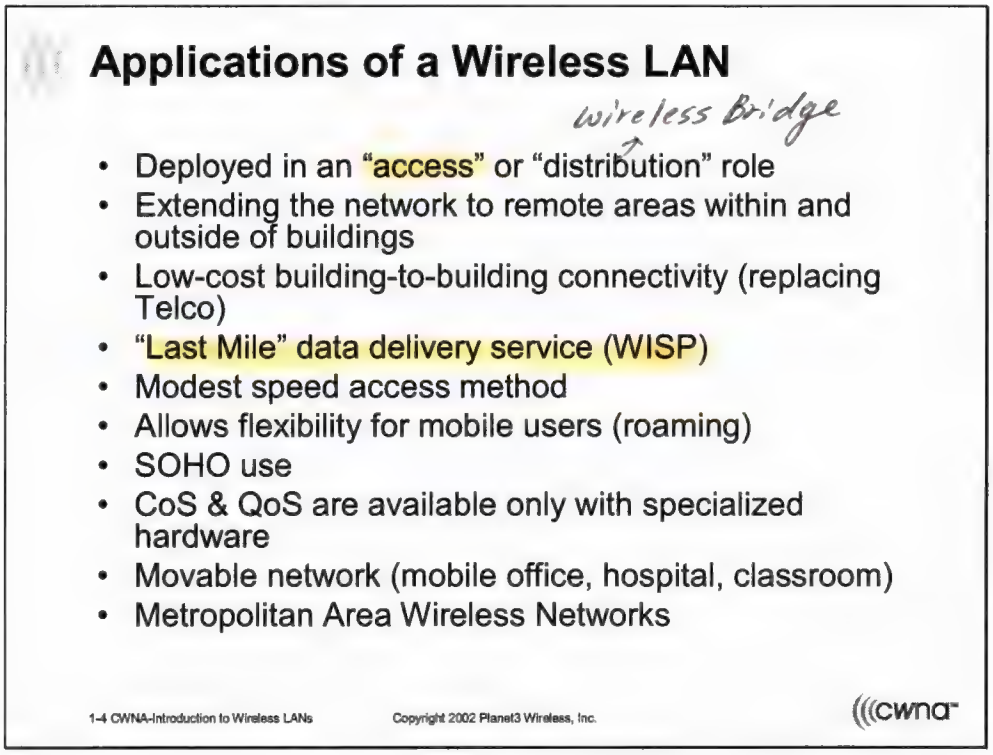
The original 802.11 standard specified medium access and physical layers for 1 and 2 Mbps wireless connectivity between fixed and portable stations within a local area. Because the technology was new, it was still cost prohibitive to implement a wireless LAN in comparison to a cabled network.

As prices of wireless LAN components dropped, rapid adoption of wireless LANs meant that enterprises would demand more features from hardware - mainly an increase in amount of data that can be transmitted over the network. The IEEE created more standards based on the original 802.11 specifications to support the needs of enterprise users.

- 802.11b - an additional standard by the IEEE for direct sequence spread spectrum (DSSS) wireless LANs, with data rates of up to 11 Mbs.
- 802.11a - an additional standard by the IEEE that allowed a wireless LAN to operate in the unlicensed 5 GHz UNII bands, with data rates up to 54 Mbps.
- 802.11g – allows for the same data rates as 802.11a, but defines use of the 2.4 GHz ISM band and requirements for backwards compatibility with 802.11b so older hardware does not necessarily have to be replaced.

Wireless network:
- Control / management frame transmit 1 or 2 Mbps
RTS/CTS
probe frames

Copyright © 2003, Planet3 Wireless, Inc.


Applications of a Wireless LAN
wireless Bridge
• Deployed in an "access" or "distribution" role
• Extending the network to remote areas within and outside of buildings
• Low-cost building-to-building connectivity (replacing Telco)
• "Last Mile" data delivery service (WISP)
• Modest speed access method
• Allows flexibility for mobile users (roaming)
• SOHO use
• CoS & QoS are available only with specialized hardware
• Movable network (mobile office, hospital, classroom)
• Metropolitan Area Wireless Networks
1-4 CWNA-Introduction to Wireless LANs
Copyright 2002 Planet3 Wireless, Inc.
cwna

Applications

Access & Distribution Roles

Because a wireless LAN does not provide functionality for routing and has slower data speeds than wired networks, they are typically deployed in an "access" role. Wireless clients gain access to the wired network using the wireless LAN. The wireless LAN infrastructure hardware is the client's first point of contact into the network.

Wireless LANs are used in a "distribution" role in building-to-building or tower-to-tower bridging scenarios. For example, if a hospital housed the main network backbone, and connected to this backbone is a wireless bridge that connects to doctor's offices in the immediate area, the wireless bridges would be considered to be playing a distribution role in the wireless network. Access is far more prevalent than distribution for wireless devices, but wireless LAN hardware can play either role.

Extending the Network

Wireless LANs become most beneficial to implement when the cost of installing cable or fiber is too great or the need to be mobile within or around a facility arises. The cost of connecting different offices, different floors of a building, or different buildings together may include:

- Labor charges

- Special permits to install/move electrical cables
- Special permits to run conduit underground between buildings
- Cabling costs
- Telco costs such as monthly ISDN or T1 charges

The installation of a wireless LAN has its own associated costs, but does not incur many of these costs, and does not take nearly as long to install or configure.

WISP

Wireless Internet Service Providers (WISP) may use wireless LANs for 'last mile' data delivery service to their customers. The communications medium that exists between a network service provider and an end user is referred to as the 'last mile'. This medium is usually seen in the form of telephone lines, cable television, and now wireless LANs.

Note As wireless LANs continue to grow in popularity, more WISPs will crop up to meet the need of 'last mile' services at lower costs than those offered by current wired solutions. Another relatively unknown player in this area is the local wireless community, wherein a person with high-speed Internet access allows other residents in a local area to connect to an open wireless LAN. More information on this subject can be found at www.freenetworks.org.

Speed

The most common wireless LAN hardware in use today is based on the 802.11b standard. Although this hardware solution is very affordable as a wireless LAN solution, it only offers a data transfer rate of 11Mbps. This solution is fine for users that do not have network intensive applications running on wireless LAN clients. Having many users trying to watch a corporate training video over the wireless network, for example, is not recommended using this technology.

Mobility

A wireless LAN solution is ideal for users who need to move around the office frequently. For workplaces where wired devices may get in the way, such as a factory production floor, a wireless solution also works well. Using wireless technologies in this manner frees users from tripping over cables or unplugging their PCs as they move about the workplace. Today's wireless LANs allow users to 'roam' from one area of wireless LAN coverage to another without losing their network connections.

Note Visit the WLANA website at www.wlana.org for a number of case studies involving wireless networks and the solutions that were implemented.

Copyright © 2003, Planet3 Wireless, Inc.

Small Office/Home Office (SOHO)

More and more homes and small businesses are creating networks every day. One of the primary reasons for this is so that users can share one connection to the Internet. The cost of entry-level wireless devices makes it very inexpensive for an individual to setup a small wireless network for file and application sharing and sharing of a broadband Internet connection.

Quality of Service & Class of Service

Today's IEEE wireless LANs offer no Quality of Service (QoS). For this reason, specialized devices called wireless LAN gateways have now, for the most part, incorporated Class of Service (CoS) configurations where different types of users can be defined. Each type of user can have an associated profile, and a given amount of bandwidth on the wireless network can be a profile parameter. The IEEE has not defined any QoS specifications into the 802.11 series of standards, but work is currently being done to address this need in future standards. Competing technologies such as ETSI's HiperLAN/2 currently address the need for QoS.

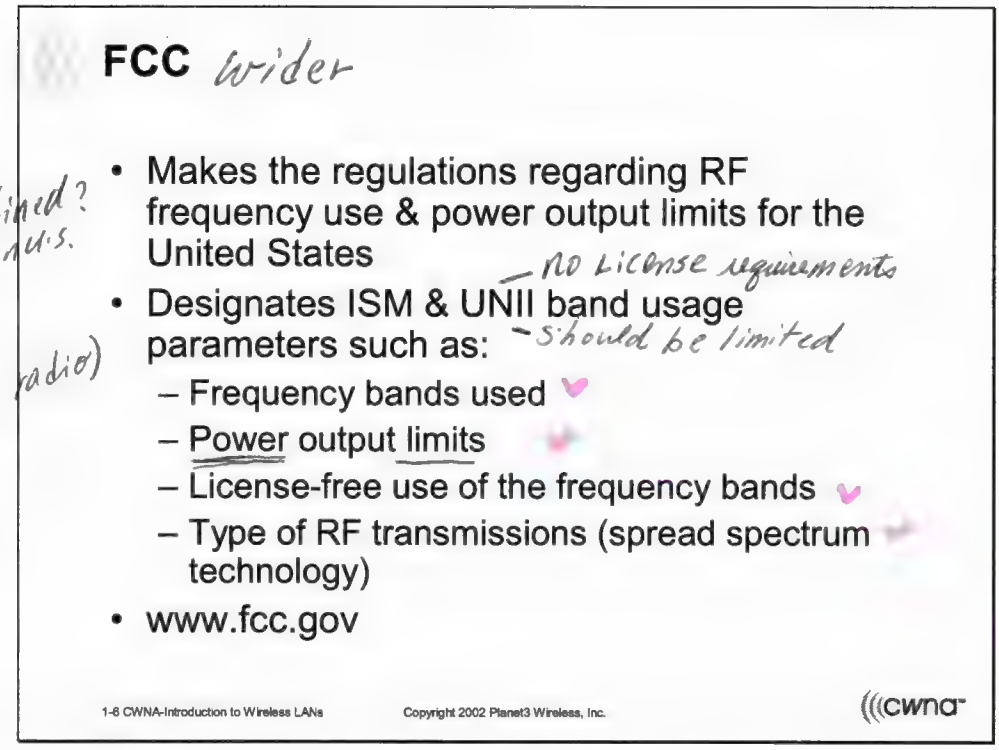
Movable Networks

As enterprises and organizations grow and add employees, they often outgrow their facilities and either move to a completely new location or lease additional space nearby. One thing that cannot be done with a wired network is to take the wiring when the organization leaves an office space. A wireless LAN allows for all of the hardware to be packed up and moved to a new location quickly and easily. At the same time the new location does not have to be fitted with nearly as much cabling. There is cabling involved with any wireless LAN, but it is minimal in comparison to a wired network.

Metropolitan Area Wireless Networks

Some municipalities may deploy access points in "hot spots" or throughout a metropolitan area for use by municipal services, including law enforcement, fire, ambulance, and other services. Mobile municipal clients can utilize the wireless connection to communicate with wired services such as municipal databases or the Internet, improving productivity.

Copyright © 2003, Planet3 Wireless, Inc.


FCC
• Makes the regulations regarding RF frequency use & power output limits for the United States
• Designates ISM & UNII band usage parameters such as:
– Frequency bands used
– Power output limits
– License-free use of the frequency bands
– Type of RF transmissions (spread spectrum technology)
• www.fcc.gov
1-8 CWNA-Introduction to Wireless LANs
Copyright 2002 Planet3 Wireless, Inc.
cwna

FCC

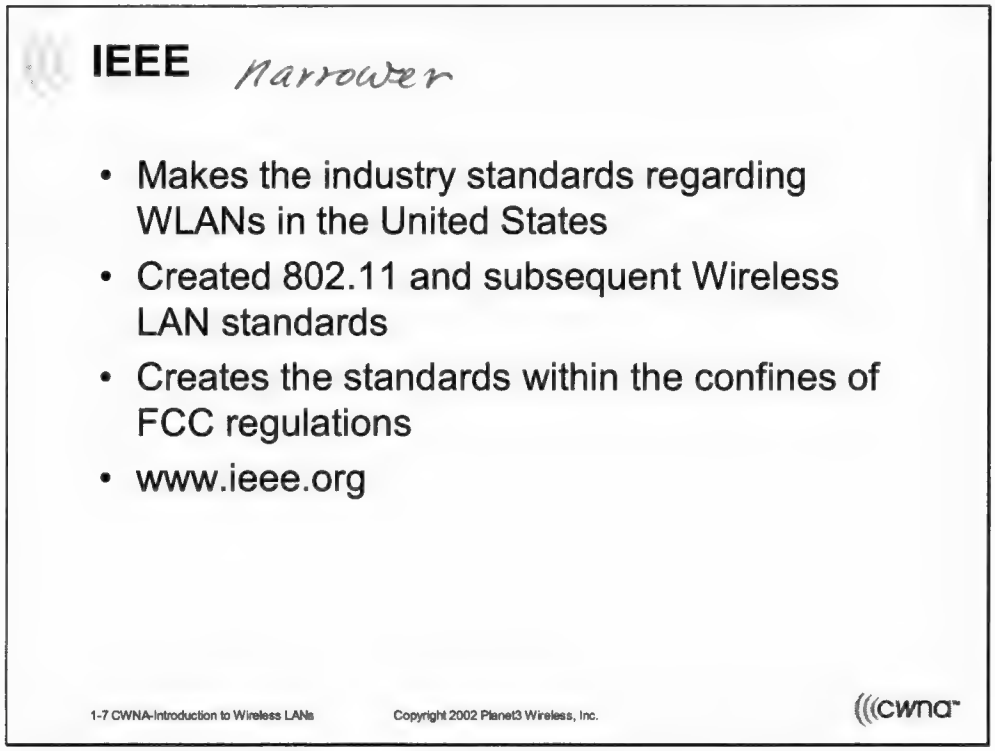
The Federal Communications Commission (FCC) is an independent United States government agency, reporting directly to congress. The FCC is charged with regulating interstate and international communications by radio, television, wire, satellite, and cable. Wireless LAN transmissions fall under FCC jurisdiction.

The FCC specifies frequencies, power output and spread spectrum techniques for wireless LAN communications. The FCC currently allows DSSS, FSSS, and other spread spectrum technologies in the frequency bands used by wireless LANs. Originally, they only allowed DSSS and FSSS technologies.

The most misunderstood fact about the role the FCC plays in the implementation of wireless LANs is that **ALL** wireless LAN systems **MUST** be certified by the FCC as a complete system and given a certification number. This certification will be accompanied by a certificate that will list the pieces of equipment and their FCC identifiers that are permitted for use with that specific wireless LAN system. All pieces of the wireless LAN setup that is used must be listed in the certificate. Understanding this requirement becomes especially crucial when dealing with amplifiers, which will be discussed in a later section.

Note Violating designated power outputs and frequencies when implementing a wireless LAN or use of a non-certified system can result in the FCC shutting down the system and/or charging the organization with very steep fines.

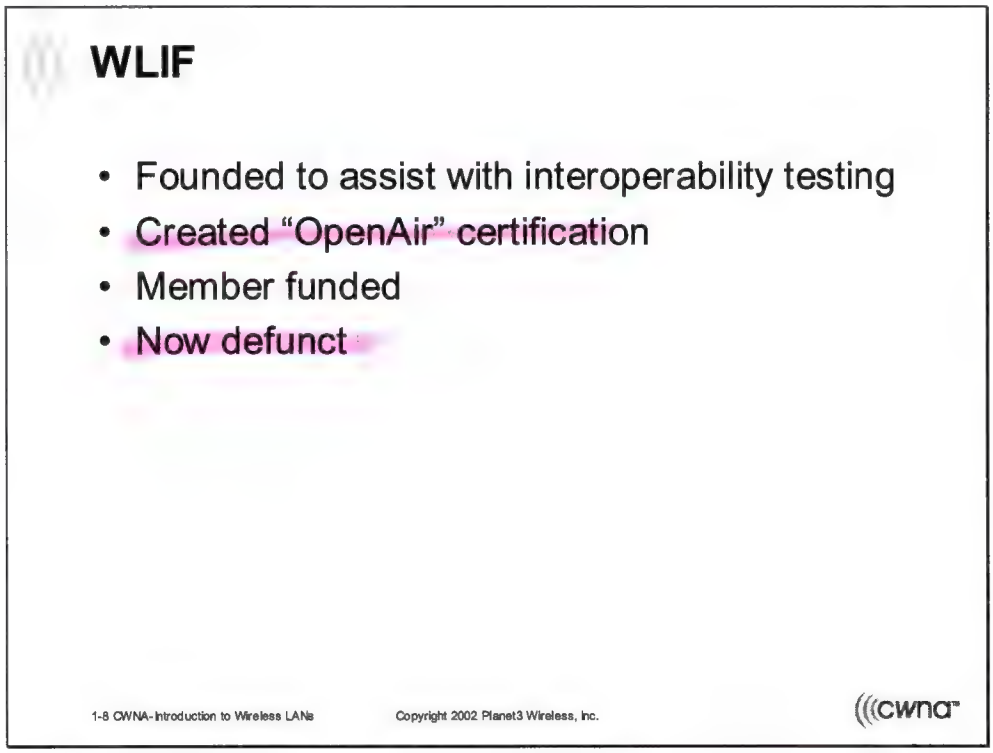
Copyright © 2003, Planet3 Wireless, Inc.


IEEE
narrower
• Makes the industry standards regarding WLANs in the United States
• Created 802.11 and subsequent Wireless LAN standards
• Creates the standards within the confines of FCC regulations
• www.ieee.org
1-7 CWNA-Introduction to Wireless LANs
Copyright 2002 Planet3 Wireless, Inc.
cwna

IEEE

The Institute of Electrical and Electronic Engineers (IEEE) is a United States based standards organization participating in the development of standards for data transmission systems. The IEEE has made significant progress in the establishment of standards for LANs, namely the IEEE 802 series of standards. The IEEE is also responsible for the newer 802.11 wireless standards.

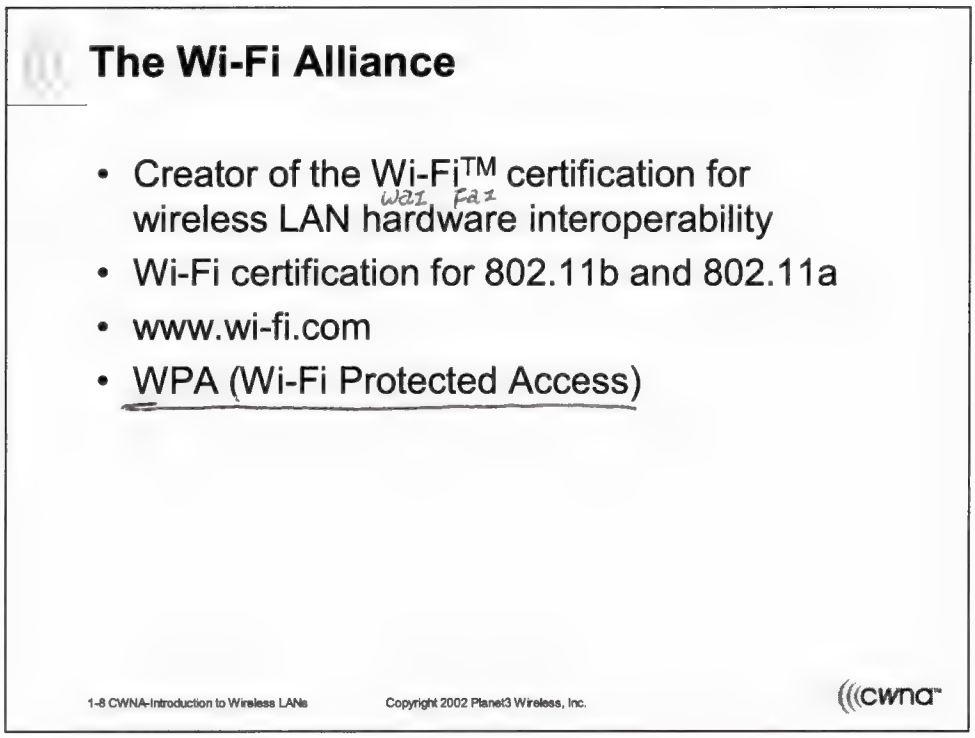
The wireless standards that are part of the 802.11 family must all adhere to the rules and regulations set forth by the FCC. These rules and regulations include the allowable frequency ranges for data transmission and power output limits within these frequency ranges. The IEEE works closely with the FCC to ensure that its standards are created within FCC regulations.



WLIF

The OpenAir standard was a standard created by the Wireless LAN Interoperability Forum (now defunct) that many wireless LAN systems were created to comply with as an alternative to 802.11. OpenAir specified two speeds - 800 kbps and 1.6 Mbps. OpenAir and 802.11 systems are not compatible and will not interoperate. Since there are currently several product lines still available that comply with the OpenAir standard, it is important that the wireless LAN administrator know that OpenAir exists; however, OpenAir is quickly losing support among vendors and no new products are being made to comply with this standard. OpenAir was the first attempt at interoperability and standardization among wireless LANs.

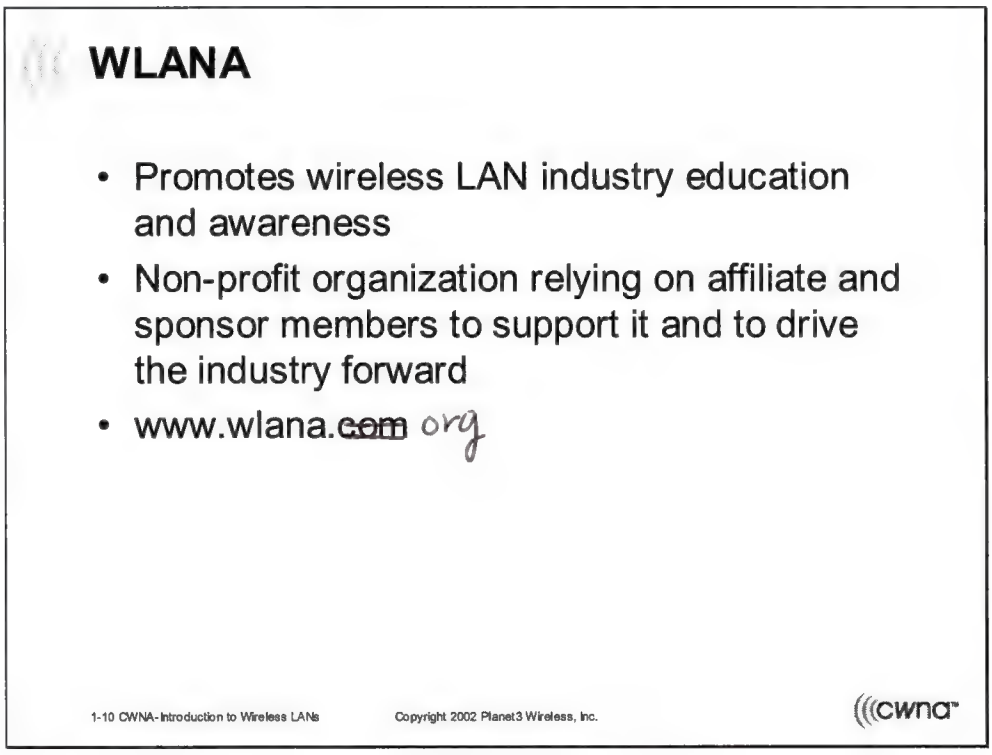
Copyright © 2003, Planet3 Wireless, Inc.


The Wi-Fi Alliance
• Creator of the Wi-Fi™ certification for wireless LAN hardware interoperability
• Wi-Fi certification for 802.11b and 802.11a
• www.wi-fi.com
• WPA (Wi-Fi Protected Access)
1-8 CWNA-Introduction to Wireless LANs
Copyright 2002 Planet3 Wireless, Inc.
cwna

Wi-Fi Alliance

The Wi-Fi Alliance was formed in 1999 with it's mission being to certify interoperability of IEEE 802.11b and 802.11a products and to promote Wi-Fi™ as the global wireless LAN compatibility standards across all market segments. When a vendor's hardware product achieves Wi-Fi™ certification, the product is certified to be in compliance with the 802.11b or 802.11a standards and interoperable among all other 802.11b or 802.11a Wi-Fi™ devices. Members of the Wi-Fi Alliance include leading wireless equipment and software providers. The Wi-Fi Alliance has contracted the testing of 802.11b and 802.11a products for certification out to various organizations since the inception of the Wi-Fi™ certification. A vendor's hardware that has passed the Wi-Fi Alliance's certification is authorized to have the special Wi-Fi™ logo on their products. The Wi-Fi Alliance maintains a list of certified hardware on its website at www.wi-fi.com.

In October 2002, the Wi-Fi Alliance announced that a new standards based solution to counteract the weaknesses in WEP would be included in all Wi-Fi products starting in early 2003. WPA (Wi-Fi Protected Access) will include both TKIP and 802.1*x* with EAP authentication--as part of all Wi-Fi certified devices starting in early 2003. This is an interim solution that is aimed at providing protection now without the need to wait for the forthcoming IEEE 802.11i standard. WPA is an extremely valuable solution that will immediately bring increased security to home and business wireless networks from the get-go by protecting against the vulnerabilities inherent with WEP. In an enterprise environment, WPA can work together with a RADIUS server to ensure mutual authentication for all wireless users. Look for WPA products for new wireless network implementations.


WLANA
• Promotes wireless LAN industry education and awareness
• Non-profit organization relying on affiliate and sponsor members to support it and to drive the industry forward
• www.wlana.com org
1-10 CWNA-Introduction to Wireless LANs
Copyright 2002 Planet3 Wireless, Inc.
cwna

WLANA

The Wireless LAN Association (WLANA) provides a clearinghouse of information about wireless local area networking, issues, and trends. It serves as a resource to customers, prospects of wireless local area products, prospects of wireless personal area products, and industry press and analysts.

The WLANA website (www.wlana.com) provides a number of white papers, reports, and case studies about the wireless market. For students looking to learn additional information about wireless LANs, the WLANA website is a good place to start.

802.11i

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

2 Radio Frequency (RF) Fundamentals

Objectives

Upon completion of this chapter you will be able to:

- Describe the behavior of RF
- Explain the variables involved with antennas and RF
- Perform RF mathematics for building FCC compliant systems

2-2 CWNA-Radio Frequency Fundamentals Copyright 2002 Planet3 Wireless, Inc.

Chapter Content

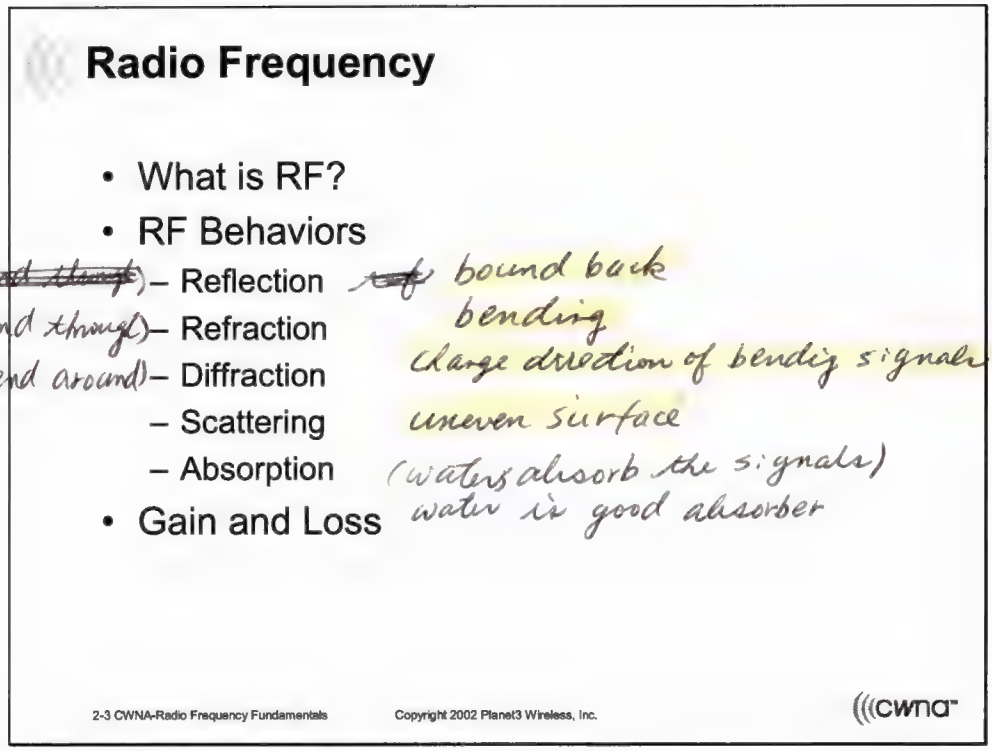
Wireless LAN hardware specifications such as signal strength are written using radio frequency terminology. For an administrator to be able to understand the attributes of a device and how devices compare, a basic understanding of RF terminology is required. When selecting hardware and cabling that will be needed to install a wireless LAN, it is also necessary to be able to compute power loss, antenna gain, and many other factors that will impact the performance of a wireless LAN.

This chapter covers the basics of RF technology and terminology. The units of measurement are discussed, and students will walk through examples of how to convert and compute using these units. Antennas are introduced along with some of their attributes. The chapter ends with a discussion of modulation and its role in radio frequency LANs.

The chapter outline follows:

- Radio Frequency
- Antennas
- RF Math

Copyright © 2003, Planet3 Wireless, Inc.



Radio Frequency

What is RF?

Wireless LAN technology is the culmination of two unrelated technologies. In order to understand how wireless LANs operate, it is important to understand both RF and networking technologies.

To demonstrate the importance of RF signal propagation behavior, it is necessary to describe the reactions that an RF signal can have to various obstacles.

RF Behaviors

Reflection - occurs when an RF signal bounces off of a smooth surface, changing the direction of the signal.

Refraction - occurs when an RF signal is bent while passing through and being reflected by a medium with a different density.

Diffraction – a change in the direction and intensity of a group of waves after passing by an obstacle. Also refers to the bending of the RF signal as it travels past or around an object.

Scattering - occurs when the RF signal strikes an uneven surface causing the signal to be scattered in such a fashion that the resultant signals are insignificant.

Copyright © 2003, Planet3 Wireless, Inc.

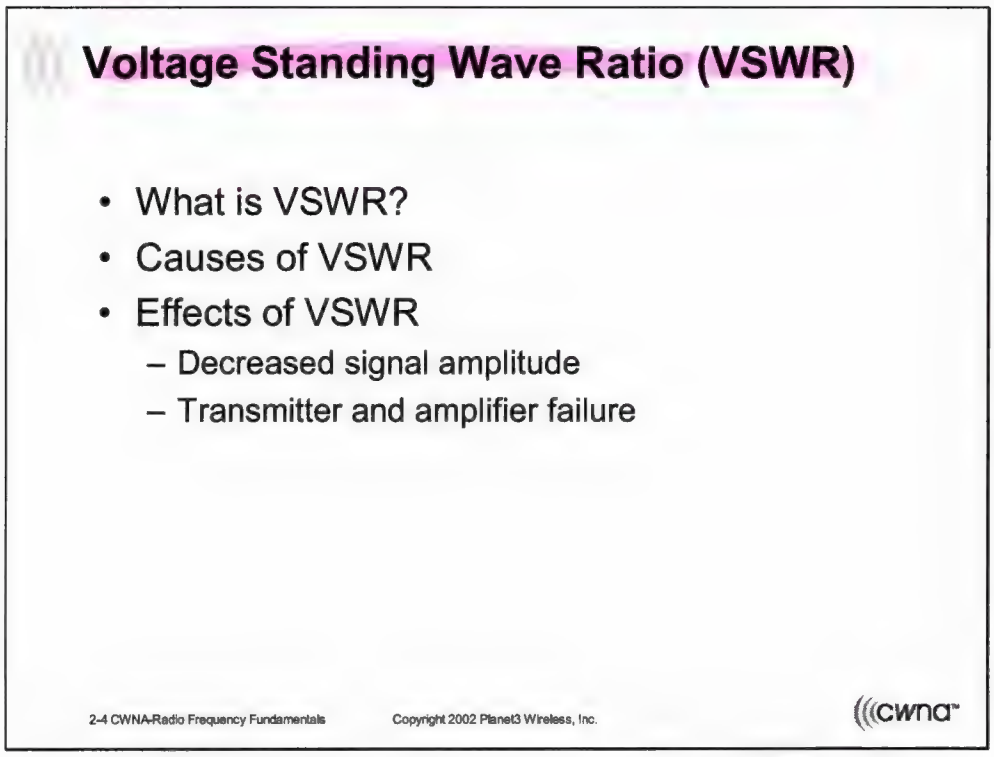
Absorption - occurs when the RF signal striking an object is absorbed into the material of the object in such a manner that it does not pass through, reflect off, or bend around the object.

Gain and Loss

Gain - the main signal flow becoming larger in amplitude due to an external power source acting upon it.

Loss - the main signal flow becoming smaller in amplitude due to an external interference source acting upon it.

Copyright © 2003, Planet3 Wireless, Inc.


Voltage Standing Wave Ratio (VSWR)
• What is VSWR?
• Causes of VSWR
• Effects of VSWR
– Decreased signal amplitude
– Transmitter and amplifier failure
2-4 CWNA-Radio Frequency Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Voltage Standing Wave Ratio

What is VSWR?

Voltage Standing Wave Ratio (VSWR, pronounced *viswar*) is caused by an impedance mismatch between connectors or devices. Impedance is a measure of the total opposition to current flow in an alternating current circuit.

Causes of VSWR

Antennas are usually located some distance from the transmitter and require a series of cables and connectors to transfer power between the two. If this series of cables has NO loss, and matches BOTH the transmitter output impedance AND the antenna input impedance, then - and only then - will maximum power be delivered to the antenna. In this case, the VSWR will be 1:1 and the voltage and current will be constant over the whole length of the series. Any deviation from this situation will cause a "standing wave" of reflected voltage to exist on the line. Most manufacturers of wireless LAN hardware provide specifications that say their equipment is specified at a VSWR of 1.5:1 or better. Military requirements are typically 1.1:1 or better.

There is always a given amount of 'return loss' (caused by VSWR) due to imperfect impedance matching between components. Return loss is the term used to describe reflected power that causes a decrease in forward power amplitude.

The goal when installing cables and connectors is to match them as closely as possible so as not to introduce any unnecessary return loss.

Effects of VSWR

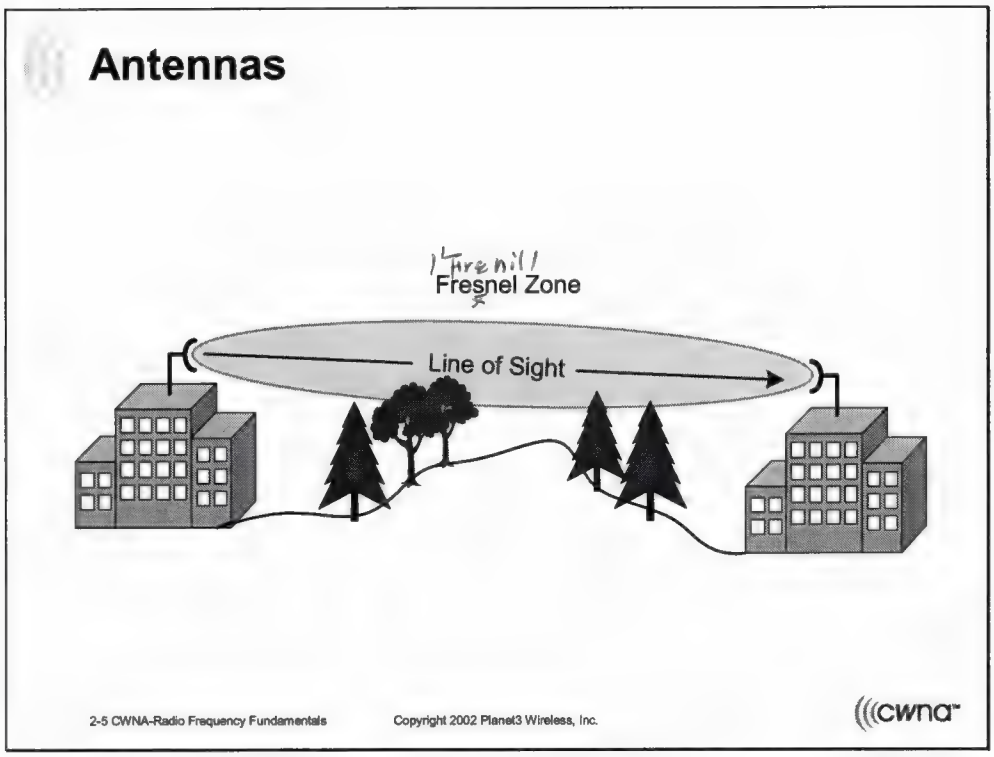
VSWR causes problems such as:

- Decreased amplitude of the main RF signal
- Transmitter and/or amplifier failure

It is IMPERATIVE that all devices, connectors, and cables in the transmission path have the same impedance (as closely as possible). Most devices used with wireless LANs have 50-ohm impedances.

Warning Do not turn on a transmitter without a termination (load) or an antenna attached – sustained VSWR at high power could damage the transmitter.

Copyright © 2003, Planet3 Wireless, Inc.



Antennas

$r = 43.3\sqrt{\frac{d}{4f}}$

Fresnel Zone

The Fresnel zone is the area surrounding the transmitted RF beam from an antenna where the radio waves spread out after leaving the antenna. Fresnel Zone size is determined by both frequency and distance between the transmitter and receiver.

Line of Sight

Line of Sight (LOS) is the ability to see one antenna from another antenna. If a person is standing next to one antenna and the other is visible, visual LOS is achieved.

Radio frequency LOS takes into consideration the Fresnel Zone. If there is visual LOS, and there are no objects intruding on the Fresnel Zone by more than 20%-40%, then RF LOS exists.

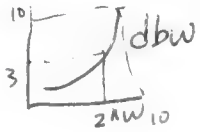
Intentional Radiator

The intentional radiator is defined as the output power of the transmitter plus the loss of cables and connectors.

Equivalent Isotropically Radiated Power

Equivalent Isotropically Radiated Power (EIRP) is the amount of power radiated from an antenna as referenced against an isotropic antenna.

dB = gain / or lost
3dBm double half.



IRP 1 mw, 10db antenna

EIRP = 10 mw.

IRP 1mw, -10db Anetena

EIRP = .1 mw
(losing the signal)

0dBm = 1mw
3dBm = 2mw
10dBm = 10mw

RF Math 0, 3, 10

The Relationship of the 10's and 3's

1 mW = 0 dBm	1 mW = 0 dBm
10 mW = 10 dBm	2 mW = 3 dBm
100 mW = 20 dBm	4 mW = 6 dBm
1W = 1000 mW = 30 dBm	8 mW = 9 dBm

gain/lose measured by dBm

2-6 CWNA-Radio Frequency Fundamentals Copyright 2002 Planet3 Wireless, Inc. ((cwna

IRP = 1mw. 16 db antenna

RF Math

EIRP = 40mw

10 db = 10mw

3 db = 20mw

6 db = 40mw

Units of measure

Watt - a standard unit of power measurement that is used to measure the rate at which power is dissipated.

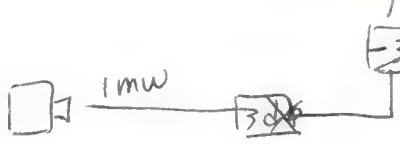
Milliwatt (mW) - standard unit of power measurement in the communications industry equating to 1/1000 of a Watt.

Decibels (dB) - in the communications industry, the decibel is used as the logarithmic expression of the ratio between two signals' output power.

dBm - decibels referenced to 1 mW (a 1 mW signal has a level of 0 dBm).

dBi - decibels referenced to an isotropic radiator (an isotropic radiator has a gain of 0 dBi).

dBd - decibels referenced to a dipole antenna vice an isotropic antenna. (0dBd = 2.14dBi).



EIRP = 4mw

topics:
- strength lose on cable
  - cheap cable is not the best always (Because "Lose").

* Link Budget

1mw
3dB
3dB

Copyright © 2003, Planet3 Wireless, Inc.

dBi = isotropics

Power conversion formulas

To convert power measurements between dBm and milliwatts a mathematical formula is needed. Two such formulas are listed below. The first is for converting power measured in mW to dBm and the second for converting power measured in dBm to mW.

$$P_{dBm} = 10*(\log(P_{mW}))$$

$$P_{mW} = (\text{inv}\log(P_{dBm}/10))$$

Power Gain & EIRP Formulas

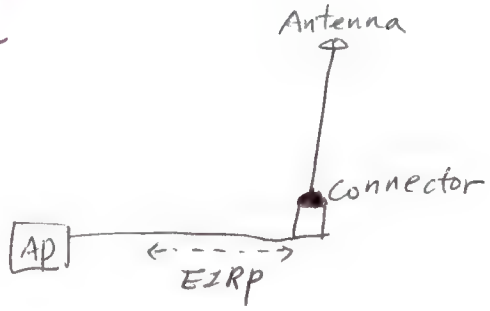
The formula used to calculate power gain is shown below. Multiplying 10 times the Log of the input power in milliwatts, divided by the output power in milliwatts, results in the power gain (measured in decibels).

Power Gain: $A_{P(dB)} = 10\text{Log}[P_{out(mW)}/P_{in(mW)}]$

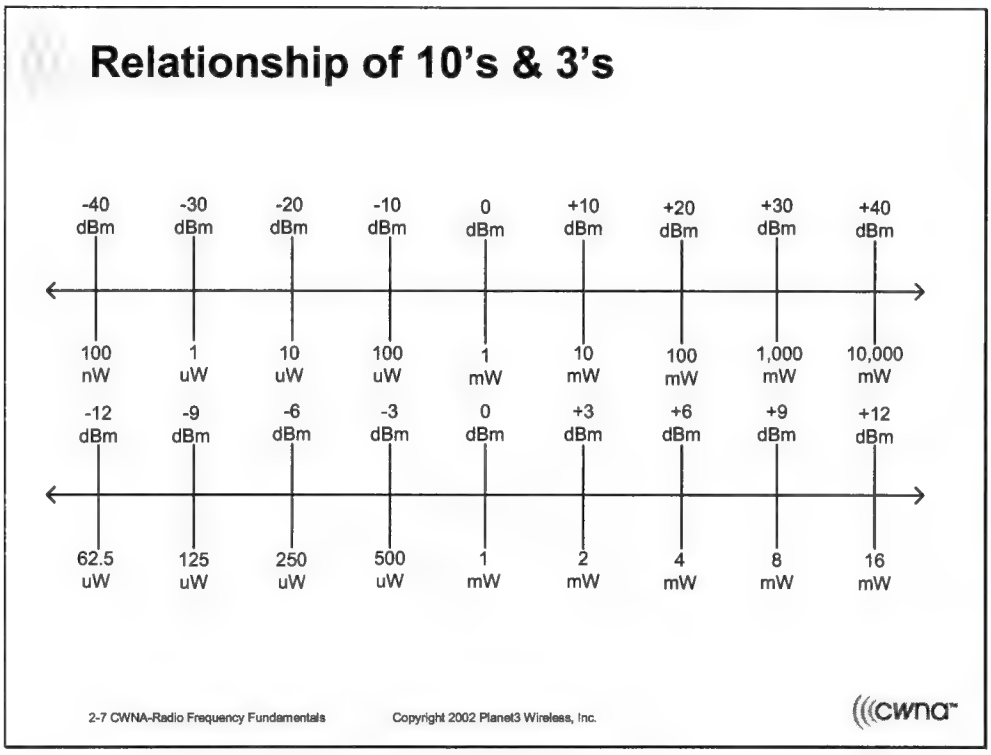
The formula used to measure EIRP (in dBm) shows that it is the sum of the transmitter power (measured in dBm) plus the antenna gain (measured in dBi) plus the cable loss (measured in -dB) as seen below.

$$EIRP = P_{xmit(dBm)} + A_{Ant(dBi)} - (A_{Cable(dB)})$$

EIRP - the power to leave Antenna



Copyright © 2003, Planet3 Wireless, Inc.



dB = in/out
Nothing more than Ratio

dB / dBm

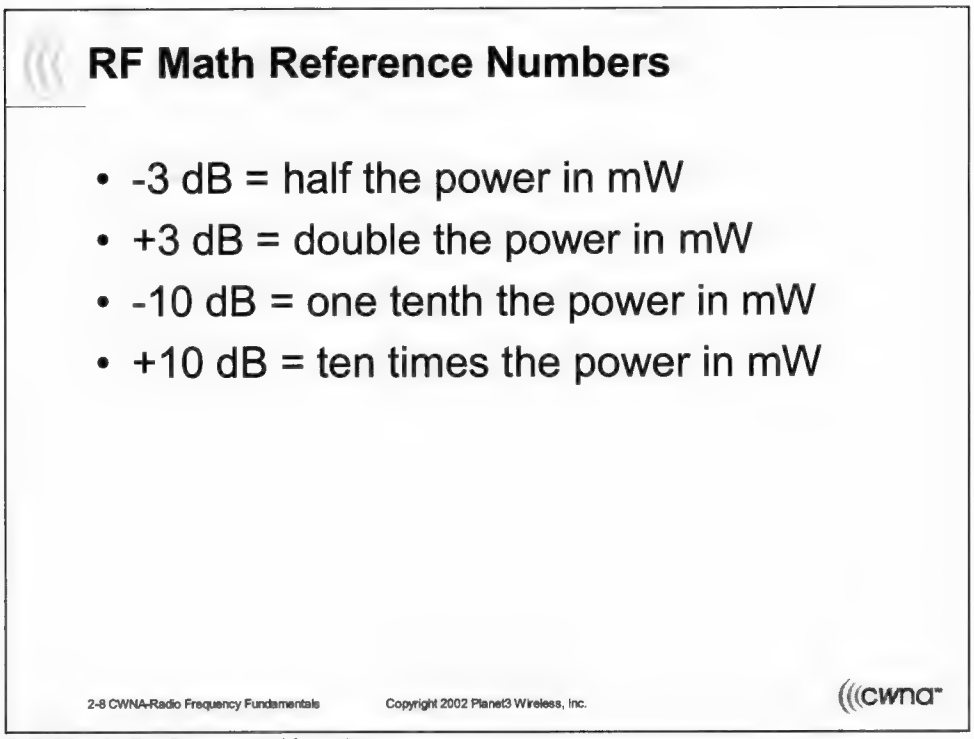
Relationship of the 10s and 3s

The beginning point of all RF math calculations involving both mW and dBm should start at the reference point of 0 dBm. Consider a horizontal line extending infinitely in both directions. In the center of this line, there is a reference point called 0 dBm. The same reference point is also called 1 mW. To the right is the "positive" direction, and to the left is the "negative" direction. As the line moves along the line to the right, positive numbers, which represent GAIN, are encountered. As the line moves along the line to the left, negative numbers, which represent LOSS, are encountered.

If a vertical line were drawn through this infinite horizontal line at the reference point, and then the top side of the line was marked with 1 mW and the bottom with 0 dBm, a good visual representation of the reference point can be found. Moving to the right to 3 dBm, directly above it would be 2 mW because a GAIN (addition) of 3 dB (+3 dB) equals a doubling of the associated power (from 1 mW to 2 mW). Conversely, moving to the left to -3 dBm, directly above it would be 0.5mW because a LOSS (subtraction) of 3 dB (-3 dB) equals a reducing of the associated power in half (from 1 mW to 0.5 mw).

Using the same example above, if moving to the right to 10 dBm, directly above it would be 10 mW because a GAIN (addition) of 10 dB (+10 dB) equals a multiplying of the power by a factor of 10 (from 1 mW to 10 mW). Conversely, moving to the left to -10 dBm, directly above it would be 0.1 mW because a LOSS (subtraction) of 10 dB (-10 dB) equals a reducing of the associated power by a factor of 10 (from 1 mW to 0.1 mW).

Copyright © 2003, Planet3 Wireless, Inc.


RF Math Reference Numbers
• -3 dB = half the power in mW
• +3 dB = double the power in mW
• -10 dB = one tenth the power in mW
• +10 dB = ten times the power in mW
2-8 CWNA-Radio Frequency Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

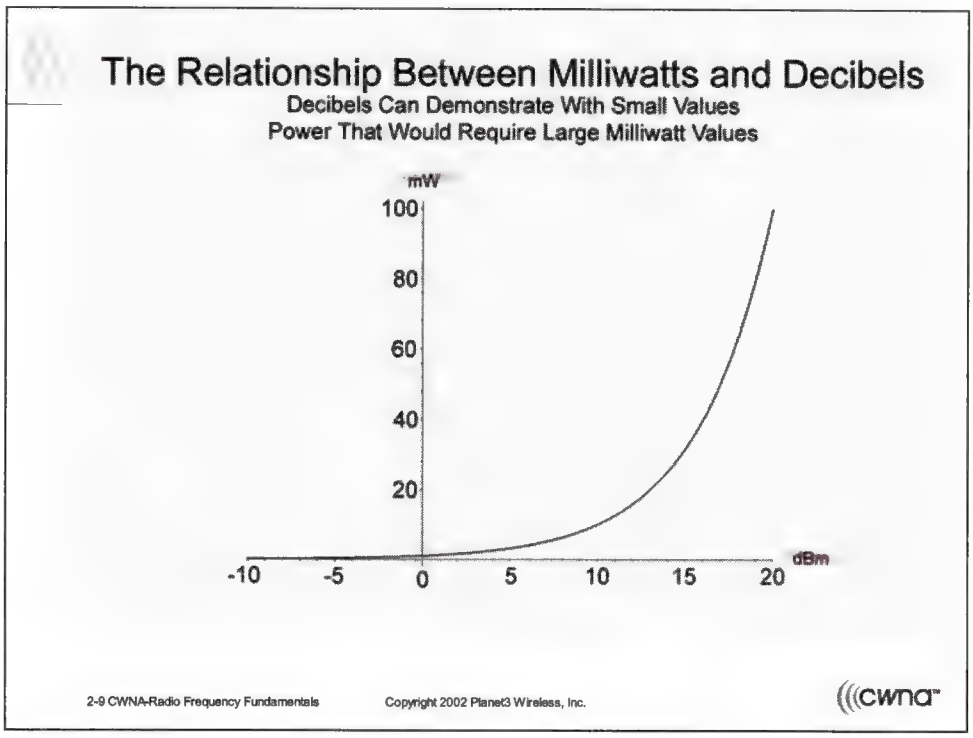
RF Math Reference Numbers

As a quick and easy reference, there are some numbers related to gain and loss that an administrator should be familiar with. These numbers are:

-3 dB = half the power in mW
+3 dB = double the power in mW
-10 dB = one tenth the power in mW
+10 dB = ten times the power in mW

When calculating power gain and loss, one can almost always divide an amount of gain or loss by 10 or 3 or both. These values give the administrator the ability to quickly and easily calculate RF loss and gain with a fair amount of accuracy without the use of a calculator. In the case where use of this method is not possible, there are conversion formulas that can be used for these calculations.

Another important point is that gains and losses are additive. If an access point were connected to a cable whose loss was -2 dB and then a connector whose loss was -1 dB, then these loss measurements would be additive and yield a total of -3 dB of loss. We will walk through some RF calculations in the coming sections to give you a better idea of how to relate these numbers to actual scenarios.



This chart displays the logarithmic relationship between decibels and milliwatts. There is no such thing as "absolute zero power" when using decibels referenced to one milliwatt (dBm). Small values represented by decibels can demonstrate power that would require long values in milliwatts.

linear scale

$10\ mW \times 2 = 20\ mW$

$10\ mW + 10\ mW = 20\ mW$

log scale

$10 \log (10\ mW) + 10 \log 2 = 10 \log (20\ mW)$

$10\ dBm + 3\ dB = 13\ dBm$

$10 \log (10\ mW + 10\ mW)$

$10 \log 10mW + 10 \log (\ldots)$

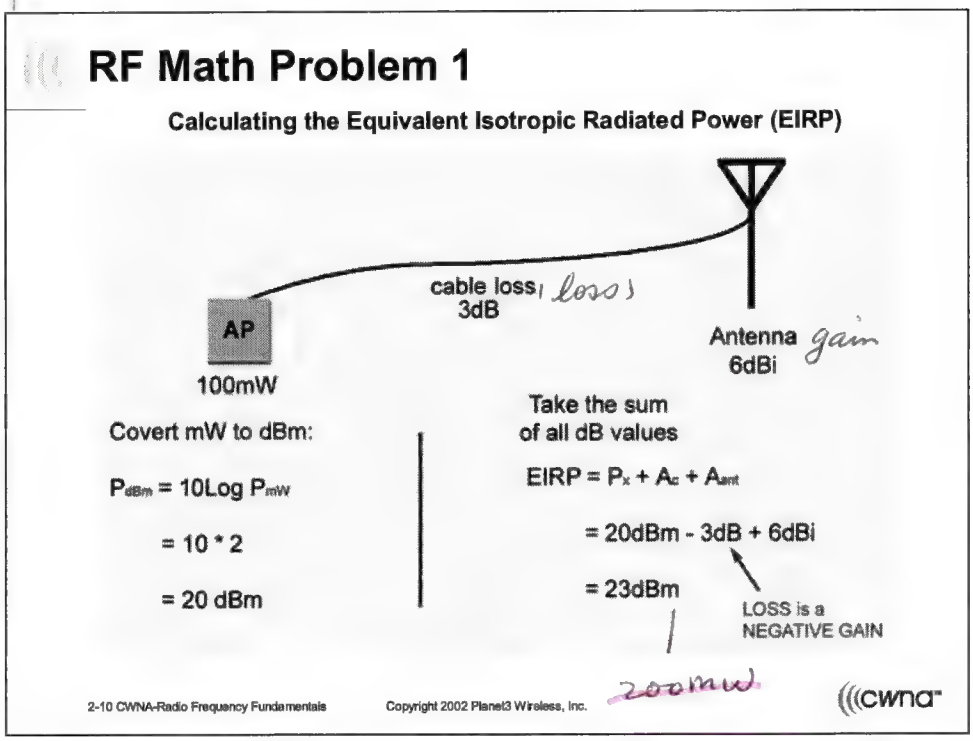
log scale

unit + unitless = unit

Copyright © 2003, Planet3 Wireless, Inc.

transmitting source dBm — relative to 1 mW } unit of power

dB — comparison
dBi — comparison } unitless



unit :

The simple calculations above, when performed, can provide the student both experience and confidence to make these calculations. This knowledge can assist individuals prior to purchasing wireless LAN equipment. Several work-through examples have been providing on the following pages with different types of problems to be solved. In each case, the longhand solution is provided to indicate how the answer was derived.

20 dBm = 100
3 dBm = 100 · 2 (double)

-3 dB

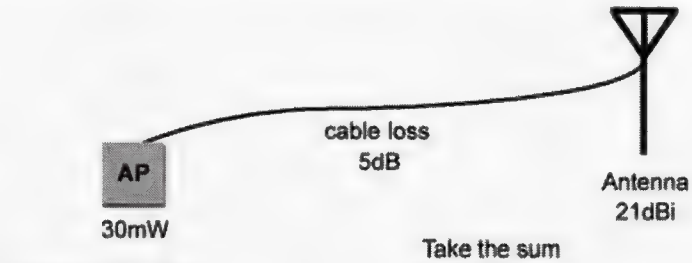
100 mW 50 mW 100 mW
200 mW

dBm — power level
dB — gain or loss of cables/amplifier
dBi — gain relative to an isotropic antenna

omni- ← I → narrow/wide as ↑ horizontal

RF Math Problem 2

Calculating the Equivalent Isotropic Radiated Power (EIRP)



Covert mW to dBm:

$P_{dBm} = 10\text{Log } P_{mW}$

$= 10 * 1.48$

$= 14.8$ dBm

Take the sum of all dB values

$EIRP = P_x + A_c + A_{ant}$

$= 14.8$ dBm - 5dB + 21dBi

$= 30.8$ dBm

LOSS is a NEGATIVE GAIN

1.2W

Copyright 2002 Planet3 Wireless, Inc.

RF Math Problem 3

Convert Decibels to Watts

$P_{mW} = \text{Log}^{-1}(P_{dBm}/10)$

$= \text{Log}^{-1}(36/10)$

$= \text{Log}^{-1}\ 3.6$

$= 3981$ mW (3.981 W)
(Estimate 4000 mW or 4 W)

$P_{mW} = \text{Log}^{-1}(P_{dBm}/10)$

$= \text{Log}^{-1}(41.1/10)$

$= \text{Log}^{-1}\ 4.11$

$= 12{,}882$ mW (12.9 W)

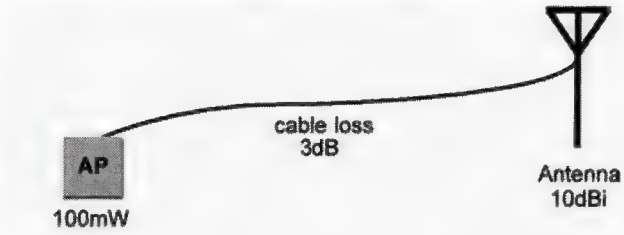
Copyright 2002 Planet3 Wireless, Inc.

1mW = 0 dbm
10dBm 10 mW
10dBm 100 mW
10dBm 1000 mW
3dBm 2000 mW
3dBm 4000 mW

Copyright © 2003, Planet3 Wireless, Inc.

RF Math Problem 4

Calculating the Equivalent Isotropic Radiated Power (EIRP)

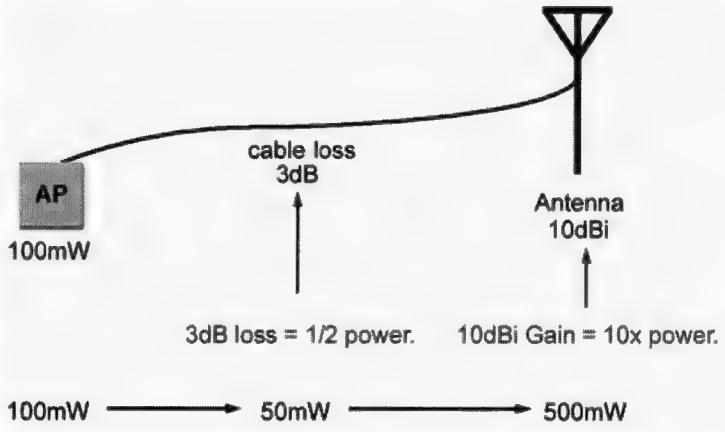


Estimate the mW-to-dBm conversion:	Take the sum of all dB values	Estimate the final dBm-to-mW conversion:
10 * 10 mW 10 + 10 dBm	$EIRP = P_x + A_c + A_{ant}$ = 20dBm - 3dB + 10dBi	10 + 10 + 10 - 3 dBm 10 * 10 * 10 / 2 mW
= 20dBm	= 27dBm LOSS is a NEGATIVE GAIN	= 500mW

Copyright 2002 Planet3 Wireless, Inc.

RF Math Problem 5

Calculating the Equivalent Isotropic Radiated Power (EIRP)



Copyright 2002 Planet3 Wireless, Inc.

Copyright © 2003, Planet3 Wireless, Inc.

RF Problem 6

An access point with a power output of 100 mW is connected to a 24 dBi directional antenna through a 10 foot length of coax with a loss of 0.5 dB/foot. Connector losses at the access point and the antenna amount to 3dB.

a) What is the Equivalent Isotropic Radiated Power (EIRP) in dBm?
b) What is the power output at the Intentional Radiator (IR) in dBm?

RF Problem 7

An access point with a power output of 23dBm is connected to an omni-directional antenna with 6 dBi gain through an 8 foot length of coax with a loss of 0.5 dB/foot. Connector losses at the access point and antenna amount to 3 dB.

a) What is the Equivalent Isotropic Radiated Power (EIRP) in mW?
b) What is the power output at the Intentional Radiator (IR) in mW?

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

3 Spread Spectrum Technologies

Objectives

Upon completion of this chapter you will be able to:

- Define spread spectrum technologies and how they are used
- Describe modulation and the different data rates
- Explain and compare FHSS and DSSS
- List the factors that impact signal throughput and range

3-2 CWNA-Spread Spectrum Technologies Copyright 2002 Planet3 Wireless, Inc.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter Content

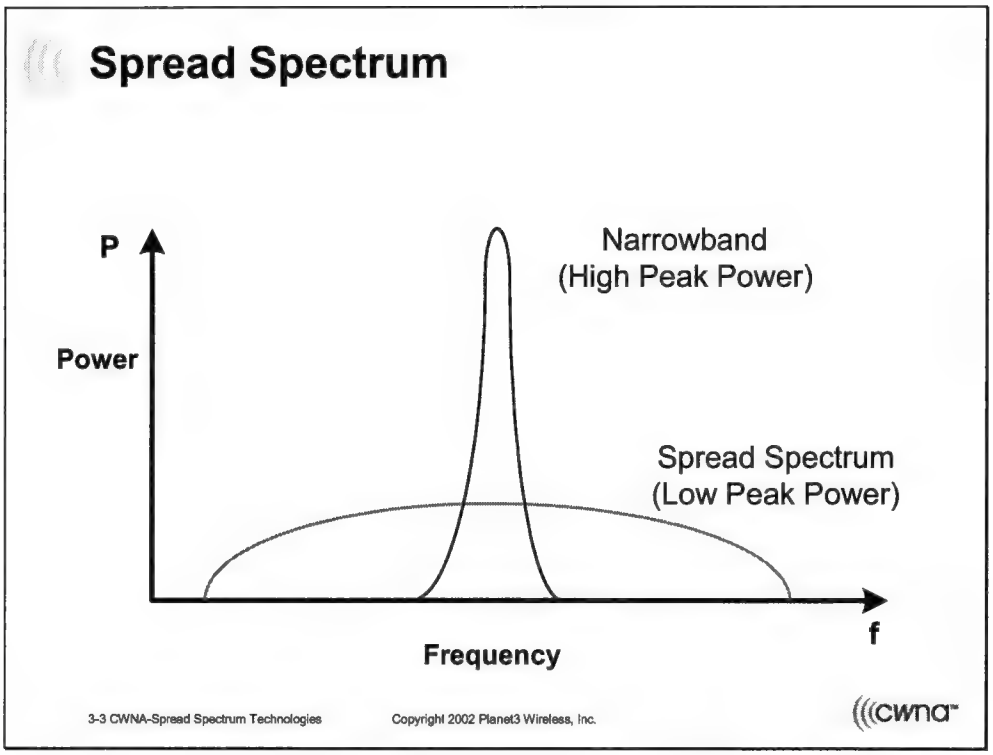
Spread spectrum technologies are an essential part of wireless networking, providing data transmission techniques that "spread" a signal's power out over a wide band of frequencies for communication.

This chapter explains the spread spectrum techniques used in wireless LANs – Frequency Hopping (FHSS) and Direct Sequence (DSSS). These two methods are compared to illustrate the advantages and disadvantages of each. Factors that affect the throughput and range of wireless transmissions are also discussed.

The chapter outline follows:

- Spread Spectrum
- Modulation Techniques
- FHSS
- DSSS
- FHSS vs. DSSS
- Throughput and Range

Copyright © 2003, Planet3 Wireless, Inc.



Spread Spectrum

Spread spectrum is a class of modulation techniques characterized by wide-bandwidth and low peak power. A set of RF signals is "spread" out over a much wider band of frequencies compared to conventional narrowband communication techniques. The primary reason for spreading the signal over a wide band of frequencies is undetectable use, which stemmed from its origin in the military.

Today, the additional characteristics of resistance to interference and low cost are the most important features of spread spectrum. Spread spectrum radios require little power to operate efficiently, and they can move large amounts of data very effectively. Radios are made very inexpensively, and have a wide range of uses in the marketplace.

With spread spectrum, data is sent on many carrier frequencies across the frequency band in use. If something were to happen to one of the carrier frequencies such as narrowband interference, then the spread spectrum radio would be able to recover lost information due to that small portion of the band being interfered with. This resistance to interference is another reason that makes spread spectrum an effective method of wireless communication.

Copyright © 2003, Planet3 Wireless, Inc.

Narrowband RF communication is a technique used by conventional radio systems such as television and AM/FM radio. These systems concentrate their power in a narrow range of frequencies to conserve as much bandwidth as possible.

Spread spectrum is used for:

- Wireless Local Area Networks (WLANs)
- Wireless Personal Area Networks (WPANs)
- Wireless Wide Area Networks (WWANs)
- Body area network (BAN)

FCC Regulations

The FCC specifies the following kinds of spread spectrum technologies for use with wireless LANs:

- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequencing Spread Spectrum (DSSS)

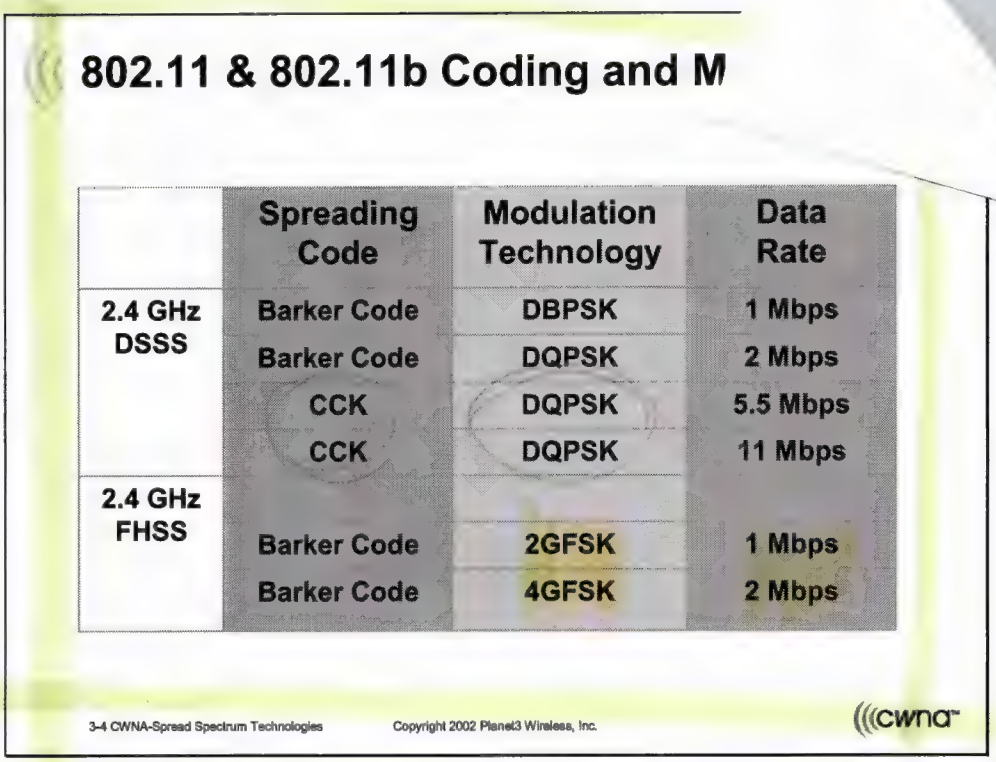
Both of these methods are used to spread the signals over a wide frequency band for use with wireless networks.

IEEE Standards

The IEEE adheres to the FCC's regulations on spread spectrum use for the 802.11 series of wireless networking standards. Both FHSS and DSSS are addressed in this series of standards.

The IEEE also specifies a technique know as Orthogonal Frequency Division Multiplexing (OFDM) to achieve higher data rates in the 802.11a and 802.11g standards. OFDM is not a spread spectrum technology like DSSS and FHSS, but rather uses multiple subcarriers operating independently and simultaneously to transmit data.

Copyright © 2003, Planet3 Wireless, Inc.



Modulation

Modulation is the process of adding data to a carrier frequency by altering the amplitude, frequency, or phase of the carrier frequency in a controlled manner. Understanding the different kinds of modulation that are used with wireless LANs is an important part of RF knowledge. It is not necessary for an administrator to understand the functionality of each type of RF modulation used with wireless LANs, but it is important to know the types of modulation that are used.

The chart above shows the details of modulation and coding types used with wireless LANs that are currently in production and being used in the market such as 802.11, 802.11b, and 802.11a. As higher data transmission speeds are needed, modulation and coding techniques change in order to provide higher throughput.

The acronyms used in the chart are

DBPSK - Differential Binary Phase Shift Keying
DQPSK - Differential Quadrature Phase Shift Keying
CCK - Complementary Code Keying
2GFSK - 2-level Gaussian Frequency Shift Keying
4GFSK - 4-level Gaussian Frequency Shift Keying
OFDM - Orthogonal Frequency Division Multiplexing
16QAM - 16-state Quadrature Amplitude Modulation
64QAM - 64-state Quadrature Amplitude Modulation

802.11a Coding and Modulation

Coding Technique	Modulation Technology	Data Rate
OFDM	BPSK	6 Mbps
OFDM	BPSK	9 Mbps
OFDM	QPSK	12 Mbps
OFDM	QPSK	18 Mbps
OFDM	16QAM	24 Mbps
OFDM	16QAM	36 Mbps
OFDM	64QAM	48 Mbps
OFDM	64QAM	54 Mbps

3-5 CWNA-Spread Spectrum Technologies Copyright 2002 Planet3 Wireless, Inc. ((cwna™

802.11a Modulation

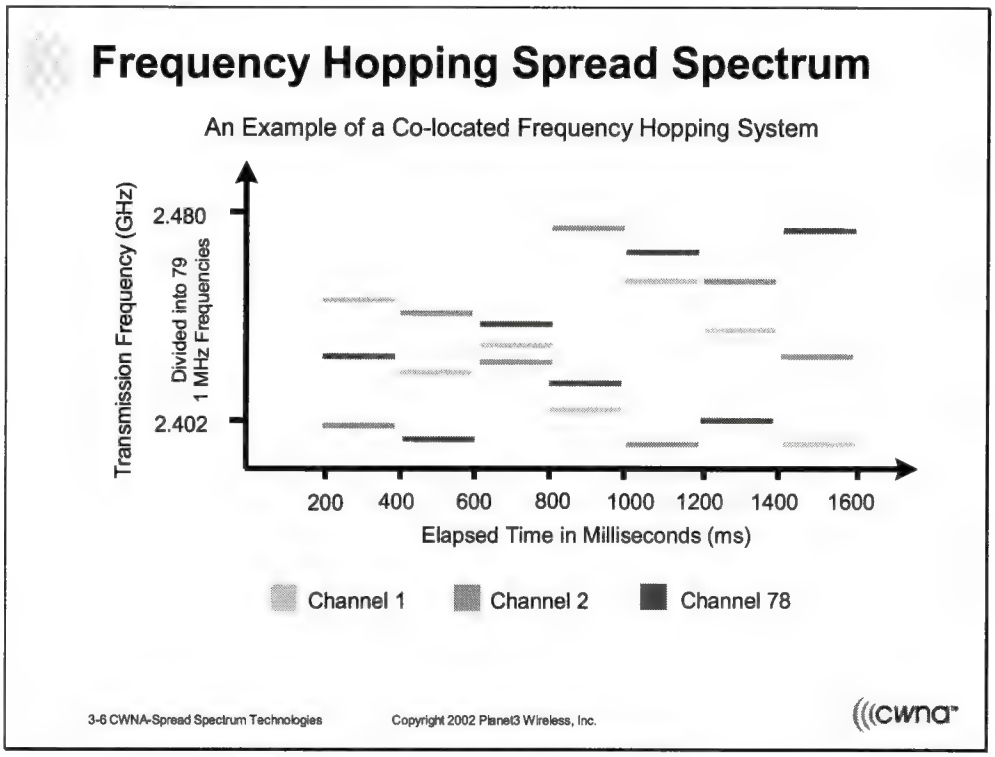
As higher transmission speeds are specified modulation techniques change in order to provide more data throughput. For example, 802.11g and 802.11a compliant wireless LAN equipment specify use of orthogonal frequency division multiplexing (OFDM), allowing speeds of up to 54 Mbps, which is a significant improvement over the 11 Mbps specified by 802.11b. The 802.11g standard provides backwards compatibility by supporting Complementary Code Keying (CCK) and even supports packet binary convolution coding (PBCC) as an option. It is important to note that 802.11g uses OFDM at higher speeds and DSSS at lower speeds. 802.11a always uses OFDM technology - not DSSS technology.

data Rate high/fast. the throuput is low

802.11a	802.11b	802.11g
OFDM	Barker Code	CCK
	CCK	PBCC

Copyright © 2003, Planet3 Wireless, Inc.

Dwell time - move from channel 1 to channel 2



Frequency Hopping Spread Spectrum

Frequency hopping spread spectrum (FHSS) is a method of sending data in which the transmission and receiving systems hop along a repeatable pattern of frequencies together. The data signal is modulated onto a set of carrier frequencies one frequency at a time in a series of "hops."

Depending on the width of a narrowband signal, narrowband and spread spectrum can co-exist in harmony in the same frequency band. The spread spectrum signals have such low power that they do not affect the narrowband signal. The narrowband signal's frequency use is so narrow that the spread spectrum system is able to recover any data lost during interference as it moves to another frequency to transmit.

Using FHSS at a rate of 1 or 2 Mbps can be achieved in the 2.4 GHz ISM band while maintaining IEEE 802.11 compliance.

Hopping Patterns

The transmission frequencies are determined by a hopping pattern (or sequence) called a "channel". The receiver must be set to the same channel as the transmitter and must listen to the incoming signal at the right time and correct frequency in order to properly receive the signal.

Standard channels are available as are custom hopping sequences depending on which manufacturer's equipment is used. The IEEE 802.11 standard specifies use of some "suggested" channels. Manufacturers may use these standard hopping sequences or program their own sequences.

FHSS is more resistant to narrowband interference due to its hopping nature across the spectrum. When FHSS encounters a narrowband signal, it simply retransmits the data once it has hopped to another carrier frequency.

FHSS is not inherently secure because the standardized hop sequence is transmitted in the clear several times per second. If a custom hopping pattern is used, it still only takes moments to track and catalog the series of hops. Only a small number of manufacturers make FHSS equipment, so trying each of their equipment in order to connect with a spread spectrum FHSS system is relatively inexpensive as well.

FCC Regulations

Current FCC regulations require manufacturers to use 75 or more carrier frequencies per transmission channel (sequence). The maximum dwell time (the time spent at a particular frequency during any single hop) is regulated to be a maximum of 400 ms, though 100-200 ms is typical in most FHSS systems today.

Note Dwell time is configurable (via software) in the radio and should be set based on the presence of interference. A shorter dwell time should be used when significant interference is present, because the amount of time in which interference can occur is reduced. If interference is not an issue, the longest dwell time available should be used to achieve the greatest throughput.

Rule Changes for FHSS

An important date to remember is August 31, 2000, which is the date the FCC created a new rule regarding FHSS to allow for wide band frequency hopping. The FCC rule changes consist of the following:

Old rules:

- 75 hops in a sequence minimum
- 1 Watt of output power in a point-to-multipoint system
- 1 MHz maximum carrier frequency bandwidth

Copyright © 2003, Planet3 Wireless, Inc.

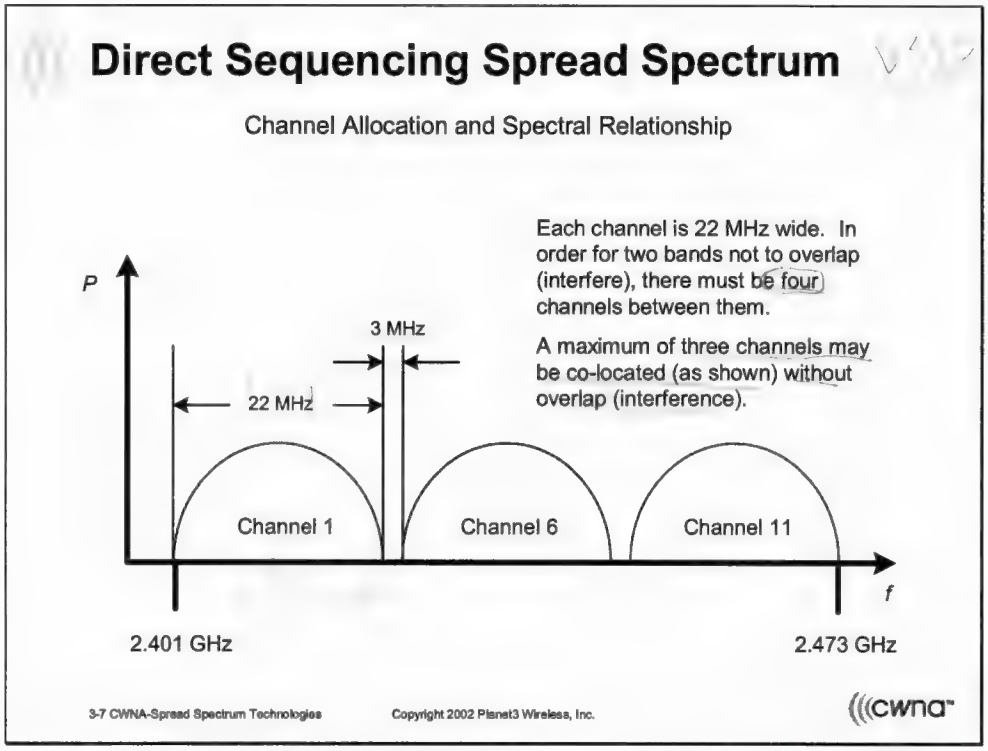
New rules: (apply to your power level)

- 15 hops in a sequence minimum
- 125 mW output power in a point-to-multipoint system
- 5 MHz maximum carrier frequency bandwidth (better frequencies more data can be carried)

The rules were changed to allow for more flexibility and increased data rates in FHSS systems. A manufacturer may create equipment that follows either one of these rules, but not both rules. There can be no mixing and matching of features of each rule on one piece of equipment.

An important note is that the new rule is flexible in that the number of hops can be 15 or more, and the carrier frequency bandwidth can be 5 MHz or less. Any combination of these two should multiply out to at least 75. For example, if a network administrator were implementing a FHSS network using equipment made according to the new rules, it would be acceptable to use 25 hops with 3 MHz carriers because that multiplies out to 75. Notice that by the old rule, 75 hops multiplied times 1 MHz carriers yields 75 MHz as well.

In gaining this flexibility and increased data throughput (from 1.6 Mbps to 10 Mbps) the big disadvantage was the reduced power output. The loss of power output from 1 Watt to 125 mW (a factor of 8) is very significant. FHSS under the new rule can have some handicaps in the enterprise environment.


Direct Sequencing Spread Spectrum
Channel Allocation and Spectral Relationship
Each channel is 22 MHz wide. In order for two bands not to overlap (interfere), there must be four channels between them.
A maximum of three channels may be co-located (as shown) without overlap (interference).
P
3 MHz
22 MHz
Channel 1
Channel 6
Channel 11
f
2.401 GHz
2.473 GHz
3-7 CWNA-Spread Spectrum Technologies
Copyright 2002 Planet3 Wireless, Inc.
cwna

Direct Sequencing Spread Spectrum

Direct sequencing spread spectrum (DSSS) is a method of sending data in which a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

The transmitting and receiving systems are both on a 22 MHz wide set of frequencies called a 'channel', using 1 MHz carriers. This 22 MHz wide set of frequencies is composed of a center frequency and the frequencies 11 MHz below and above the center frequency. For example, the center frequency of the first available DSSS channel is 2.412 GHz. This shows us that channel 1 is comprised of frequencies from 2.401 GHz to 2.423 GHz.

DSSS is fast and inexpensive. DSSS equipment complying with the 802.11 standard has data rates of 1 & 2 Mbps. Equipment complying with the 802.11b standard works at 11 and 5.5 Mbps, and has backwards compatibility with 802.11 devices at 2 & 1 Mbps. Rates up to 54 Mbps are available using the new 802.11g and 802.11a standards. The 802.11a standard specifies operation in the 5 GHz UNII bands and OFDM technology, which differs from DSSS. The 802.11g standard specifies operation in the 2.4 GHz ISM band using DSSS up to 11 Mbps for compatibility with 802.11b and OFDM for higher data rates.

Copyright © 2003, Planet3 Wireless, Inc.

DSSS technology is not inherently secure (although it was once believed to be) due to DSSS radios being widely available on the market. The military used both FHSS and DSSS for covert communication because spread spectrum was difficult to detect, but that is not the case today. The spread spectrum technologies themselves would seem secure in how they are designed, but the fact that anyone who has one or more radios capable of receiving DSSS or FHSS communications can detect a spread spectrum transmission makes these communications far less secure than they once were.

Co-location of DSSS

According to the IEEE 802.11 standard, DSSS can use 3 non-overlapping channels (1, 6, 11) allowing for up to 3 transmitters in a 2.4 GHz co-located environment. According to the IEEE there are 11 U.S. channels available for use in the 2.4 GHz ISM band. Co-location is defined as having multiple access points put into the same physical area, but configured for different operating channels so as not to interfere with each other. Co-location of access points is sometimes necessary in order to achieve a given amount of throughput for a set of users.

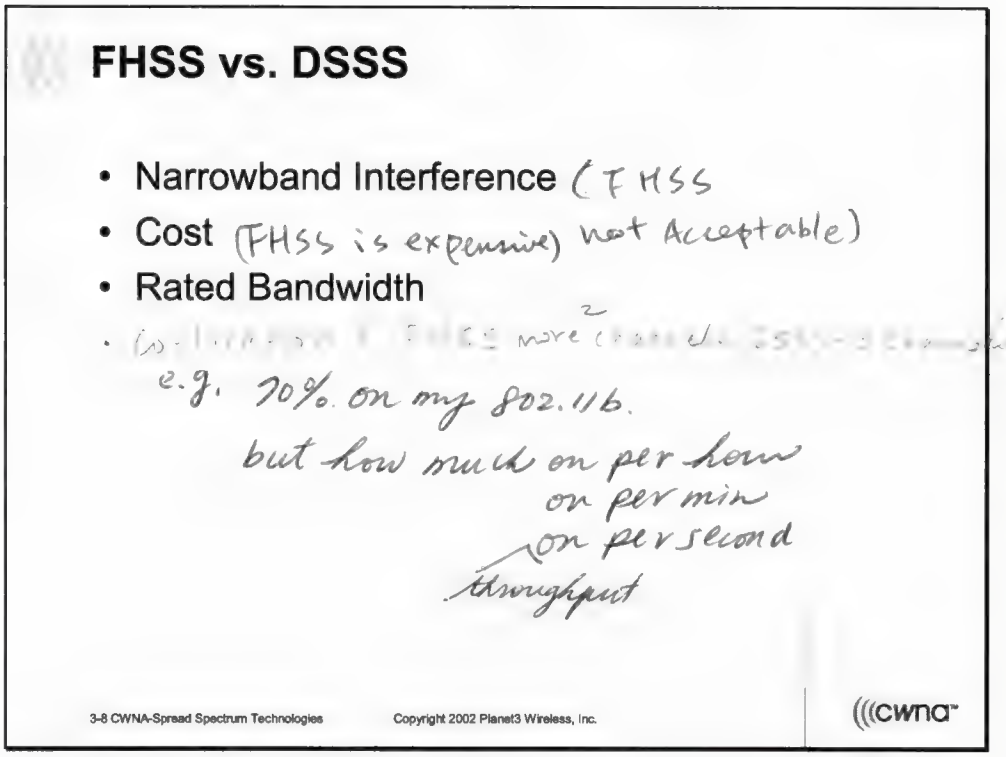
There are, in theory, 3 non-overlapping channels. The reason we use the word "theory" is because even though there is 3 MHz of channel separation between these three non-overlapping channels, viewing all three channels being used simultaneously on a spectrum analyzer (a device that gives a visual representation of frequency use in a given frequency spectrum) shows that they do actually overlap somewhat due to sidebands. This overlap is dependent on power output and proximity of the transmitting devices.

Channels with 6 MHz or more of frequency separation are typically safe to use in a co-location environment. Co-locate three access points only when absolutely necessary. Co-locating only two access points in an area will allow greater channel separation and assures no adjacent channel interference (the interference between bands positioned directly beside each other in the frequency spectrum).

DSSS Channel Frequency Assignments

Channel ID	IEEE Channel Frequencies GHz	ETSI Channel Frequencies GHz
1	2.412	N/A
2	2.417	N/A
3	2.422	2.422
4	2.427	2.427
5	2.432	2.432
6	2.437	2.437
7	2.442	2.442
8	2.447	2.447
9	2.452	2.452
10	2.457	2.457
11	2.462	2.462

Copyright © 2003, Planet3 Wireless, Inc.



FHSS vs. DSSS

Narrowband Interference

Frequency hopping is less susceptible to narrowband interference due to frequency diversity and a larger set of transmitting frequencies. DSSS is very susceptible to narrowband interference since it transmits over all twenty-two carrier frequencies simultaneously. If a source of narrowband interference were transmitting across a 3 MHz section of the ISM band, that would be a significantly larger percentage of the 22 MHz that DSSS uses than the 79 MHz that FHSS uses.

Also, FHSS moves off of the interfering frequency with each hop, lessening the effects of interference. For these reasons, FHSS more easily copes with narrowband interference. With a DSSS system, interference on the selected frequencies will prevent all data transfers on those frequencies. Interference of this nature is a significant problem for DSSS systems.

Cost

FHSS systems are typically more expensive than DSSS systems. DSSS has the added benefit of an interoperability standard called Wi-Fi™ that certifies equipment to be compatible with other 802.11b equipment. The popularity of 802.11b compliant systems (due mostly to high data rates and ease of configuration) has increased the demand to the point at which prices of this type of equipment have decreased considerably. New-in-the-box 802.11b compliant (11 Mbps) PC cards can be found for as little as $50. Before the 802.11b standard was implemented, it was not uncommon to pay $400 for one wireless PC Card.

Copyright © 2003, Planet3 Wireless, Inc.

Rated Bandwidth

The IEEE 802.11 standard specifies 1 and 2Mbps for FHSS and DSSS. There is another standard known as OpenAir that specifies FHSS speeds at 800 kbps and 1.6 Mbps. There are manufacturers that make proprietary FHSS systems that both comply with IEEE 802.11 (1 & 2 Mbps) and have modes for 3 Mbps or more. Some manufacturers have released products complying with the FCC's 08/31/2000 ruling on wide band frequency hopping that have a rated bandwidth of up to 10 Mbps. The HomeRF organization published the specifications for using wide band frequency hopping as "HomeRF 2.0." HomeRF 2.0 is backwards compatible to HomeRF 1.0 because it supports 10 Mbps and 5 Mbps speeds in addition to speeds of 1.6 Mbps and 800 kbps. HomeRF 1.0 was OpenAir compliant.

DSSS has a rated bandwidth of 11 Mbps per the 802.11b standard, but has a typical throughput of 50% of the rated bandwidth (5.5 Mbps). 802.11b compliant devices can fall back between 11, 5.5, 2, & 1 Mbps speeds in order to be backwards compatible with IEEE 802.11 devices and to extend reach of the connection (the slower the data rate, the further the connection will reach).

Co-location

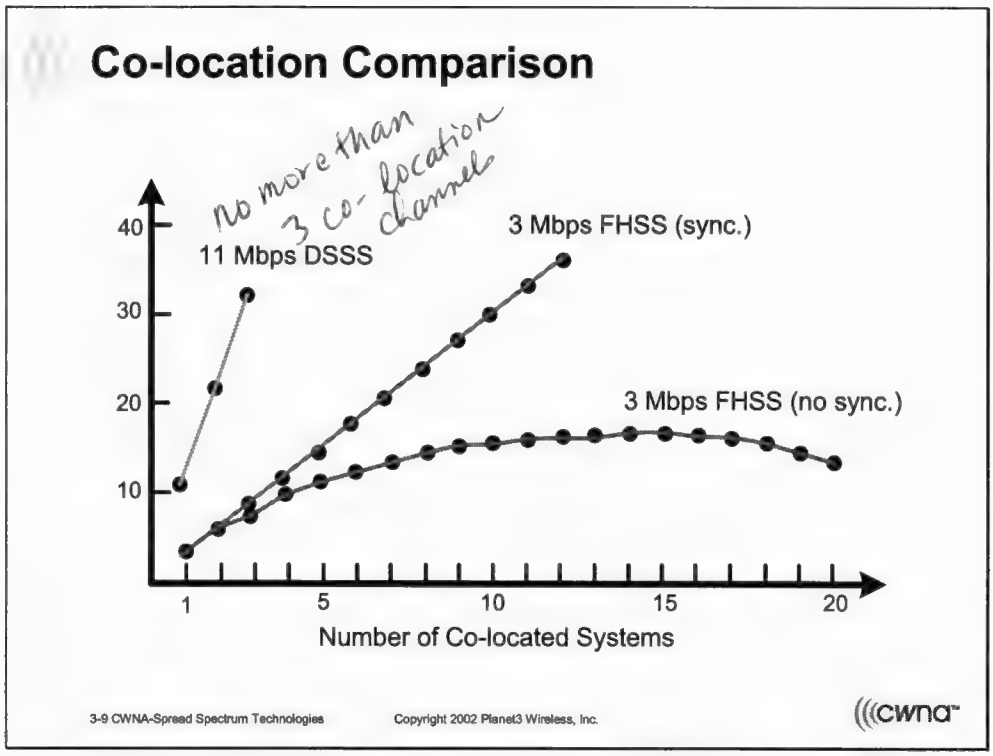
Many FHSS systems can be co-located in the same space without significant collisions, whereas with DSSS, only three such systems may be co-located.

Typically, no more than 12 synchronized FHSS access points may be co-located because radios implemented in today's systems do not provide synchronization support for more than 12. When FHSS systems are synchronized, there are no collisions between the access points. The FHSS systems coordinate the sending of frames across carrier frequencies so as not to interfere with each other. Without synchronization, 15 co-located systems will normally be the maximum before collisions become so significant that considerable throughput is lost. Theoretically, 79 FHSS radios could be co-located and synchronized (since there are 79 carriers specified for use by the IEEE), but this is unfeasible by today's standards due to cost and configuration complexity.

With DSSS systems, co-location is a matter of simultaneously implementing up to three access points configured for non-overlapping channels. Channels 1, 6, and 11 are the three channels specified for this use.

As an example of comparison, if 15 non-synchronized IEEE 802.11 compliant FHSS access points were co-located, the theoretical data rate would yield a maximum of 30 Mbps (15 x 2 Mbps = 30 Mbps). The problem with this scenario is that 15 access points, cabling and mounting equipment, installation and configuration of these 15 access points would be extremely expensive. Using DSSS, three co-located access points would yield an even higher data rate of 33 Mbps (3 x 11 Mbps = 33 Mbps) which would cut costs by approximately 5 times. Since the data throughput on these systems is about the same (50% of rated bandwidth), DSSS makes a much more economically sound business case.

Copyright © 2003, Planet3 Wireless, Inc.



Throughput and Range

Throughput

Throughput in a wireless LAN is based all of the following factors.

- Interference
- Use of WEP (Wired Equivalent Privacy)
- Distance between transmitter & receiver
- Manufacturer's hardware limitations
- Proprietary protocols
- Frame size
- Use of fragmentation
- Use of RTS/CTS protocol (discussed in PHY/MAC Layer section)
- Number of simultaneous users accessing the medium
- Use of VPN tunnels
- Type of Spread Spectrum technology in use (doesn't affect the range)
- Use of polling
- Receiver sensitivity

Copyright © 2003, Planet3 Wireless, Inc.

The throughput that can be achieved from FHSS vs. DSSS is not easily determined because it will depend on the particular network implementation as well as all of the factors mentioned above.

Range

The range of a signal depends on:

- Output power of the transmitter
- Antenna gain and the type of antenna used
- Physical environment and surroundings
- Transmission frequency used

RF signals can also be influenced by the frequency of the transmission. For example, a 900 MHz transmission has a greater range than a 2.4 GHz transmission (at the same output power), and both 900 MHz and 2.4 GHz transmissions have a greater range than a 5 GHz transmission (900 MHz, 2.4 GHz, and 5 GHz bands are used in wireless LAN communication).

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

4 Wireless LAN Infrastructure Devices

Objectives

Upon completion of this chapter you will be able to:

- Configure, install, and manage wireless infrastructure devices
- Configure, install, and manage wireless client devices
- Configure, install, and manage the different types of wireless gateways

4-2 CWNA-Hardware Management

Copyright 2002 Planet3 Wireless, Inc.

Chapter Content

There are many pieces of hardware that make up a wireless network. From small, inexpensive $10 cable adapters to enterprise wireless gateways that cost thousands of dollars, no two installations may require the exact same equipment or configuration. Because business needs vary for every organization, wireless LAN manufacturers offer a variety of solutions and types of equipment in an effort to meet any type of configuration that may be required.

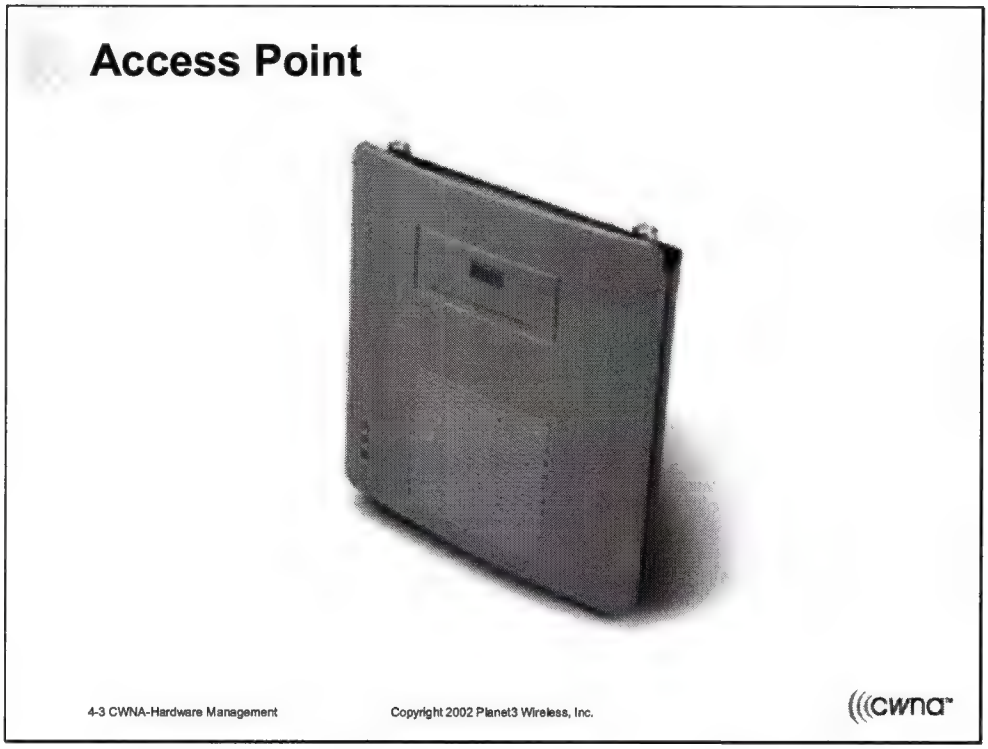
This chapter introduces the hardware that is used to create a wireless LAN, and how that hardware is installed, configured, and managed. Students will be shown the types of devices commonly found in a wireless LAN and the application of each device.

The chapter outline follows:

- Infrastructure Devices
- Wireless LAN Client Devices
- Wireless LAN Gateways

Copyright © 2003, Planet3 Wireless, Inc.

Infrastructure Devices



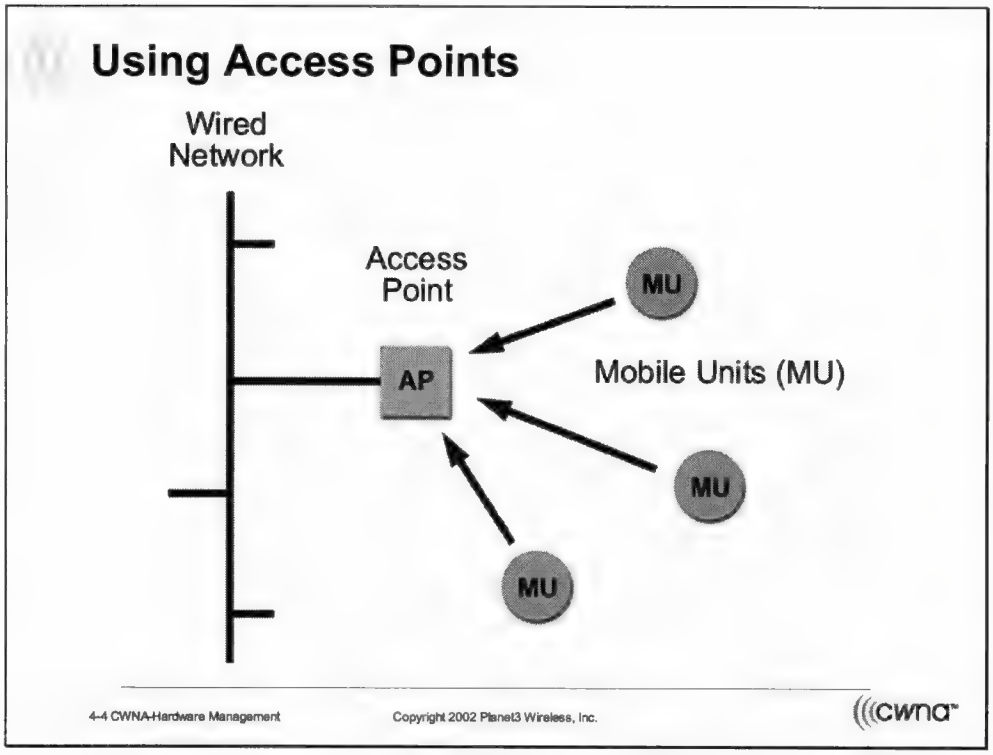
Access Points

An access point (AP) is a device that allows wireless client connectivity into the wired portion of a network. An access point is a half-duplex device with intelligence equivalent to a sophisticated Ethernet switch. Access points are considered portals – devices that connect 802.11 networks to 802.3 or 802.5 networks.

Access Point Options

Access points can vary in the options available with the hardware. Manufacturers add different features that can affect the price of the unit and its performance. Some of the options that may be available with a unit are:

- Fixed or Detachable Antennas (with or without diversity)
- Advanced Filtering Capabilities (MAC or Protocol)
- Removable (modular) radio cards
- Multiple Radio capability
- Variable output power
- Varied types of wired connectivity (10baseTx, 10/100baseTx, 100baseTx, 100baseFx, etc.)



Using Access Points

The diagram above illustrates where the access point fits into the network. On an existing wired network, the access point plugs into an existing switch or hub to be able to link to the network. Mobile units (MU) can include:

- Laptop computers
- Handheld devices such as scanners or PDAs
- Stationary computers

MUs communicate with the access point to gain network access. This setup is one of the fastest and least expensive methods to add wireless users to the network because the amount of hardware needed equates to purchasing a single access point and one or more client devices, depending on the number and type of users.

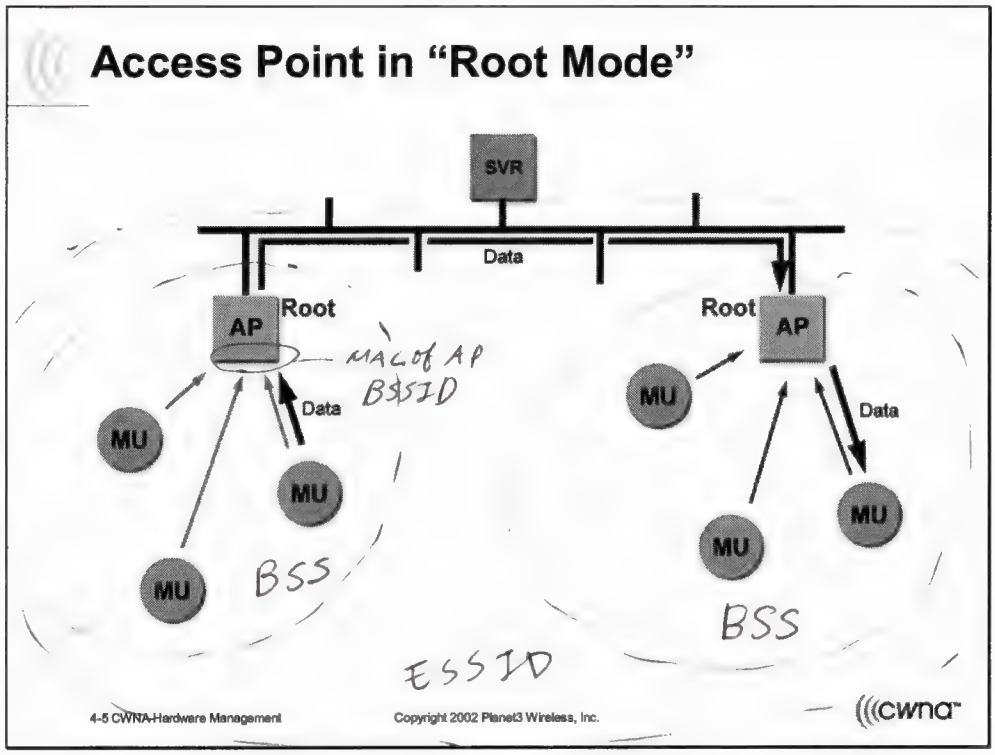
Setup and Installation

Access points can be managed and configured in many different ways. Some units may support terminal emulation sessions (telnet) while others may support web browser access (http). Some manufacturers offer custom configuration and management software. SNMP application support is featured in some models, and others may even have a legacy serial or USB port for access. It is important to choose an access point compatible with the network's management systems and methodology.

Copyright © 2003, Planet3 Wireless, Inc.

wait before the packets are transmitting:

- RTS
- internet spacing



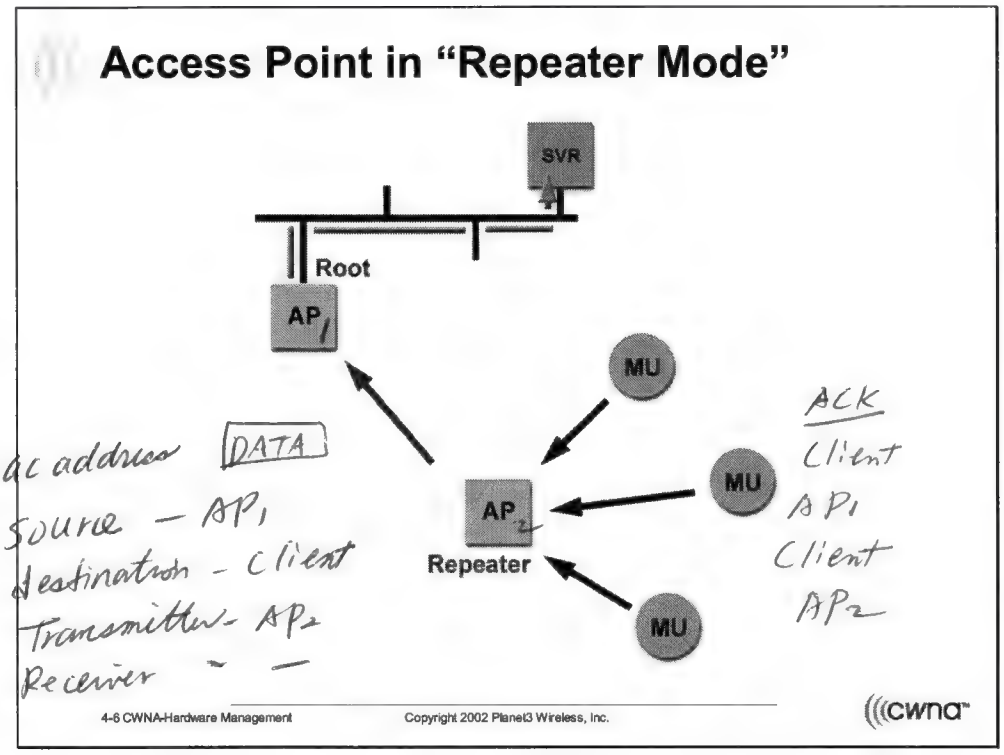
Access Point Communication

Access points communicate with other access points in one of three ways:

1. Root Mode
2. Repeater Mode
3. Bridge Mode

Root Mode

In root mode, access points communicate with each other over the wired segment of the network. As can be seen in the diagram above, the mobile units of one access point transmit data to the access point they connect to. The access point then takes that data and passes it to the wired network backbone where it is sent to a different access point. That access point then transmits the data to a listening mobile unit on the other end. This configuration could be used when there are different wireless segments on the network, where one or more access points do not have the coverage area or capacity to handle all of the users.



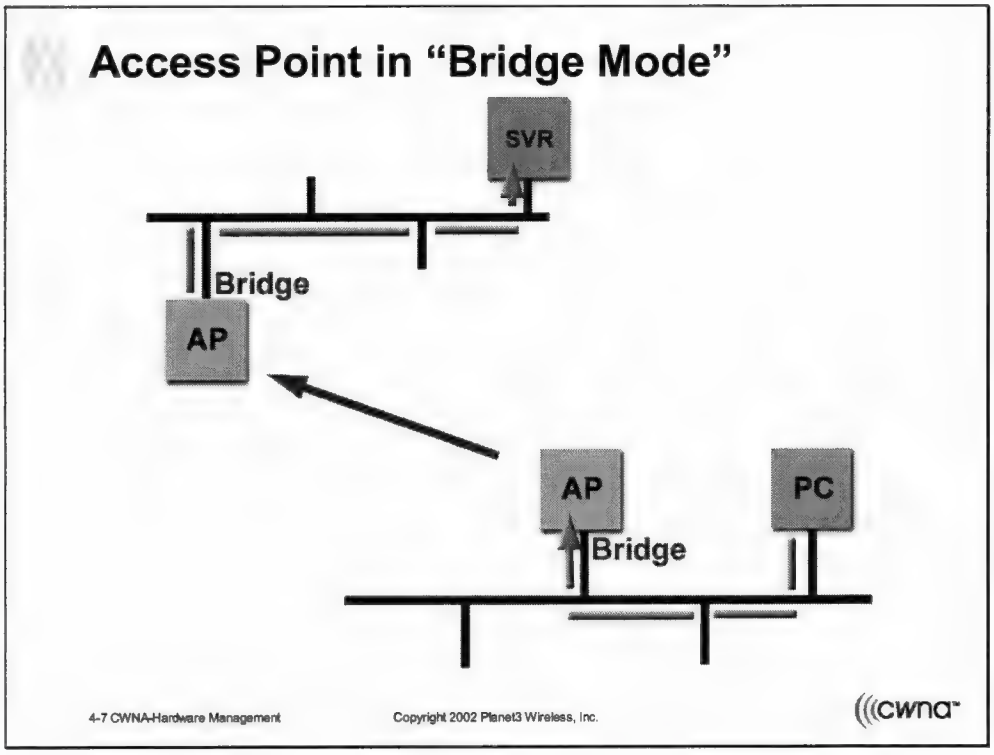
Repeater Mode

In repeater mode, an access point is responsible for handling the requests from mobile units and repeating that data to another access point that is connected to the wired network. This configuration could be used where one access point would not have the range to support distant mobile units. Instead, one access point is situated close to the mobile units and the other is connected to the wired network, with the access points communicating the data between each other. This type of configuration might be used when wiring is not available to some of the access points.

It is a good idea to avoid using access points in repeater mode whenever possible. Throughput through a repeater access point is much less than throughput though an access point in root mode because the radio must use the same shared bandwidth as the users (client devices) to repeat the user data to the upstream access point. It is never a good idea to string a series of repeater-mode access points in series due to possible data corruption over the series of hops back to the root access point.

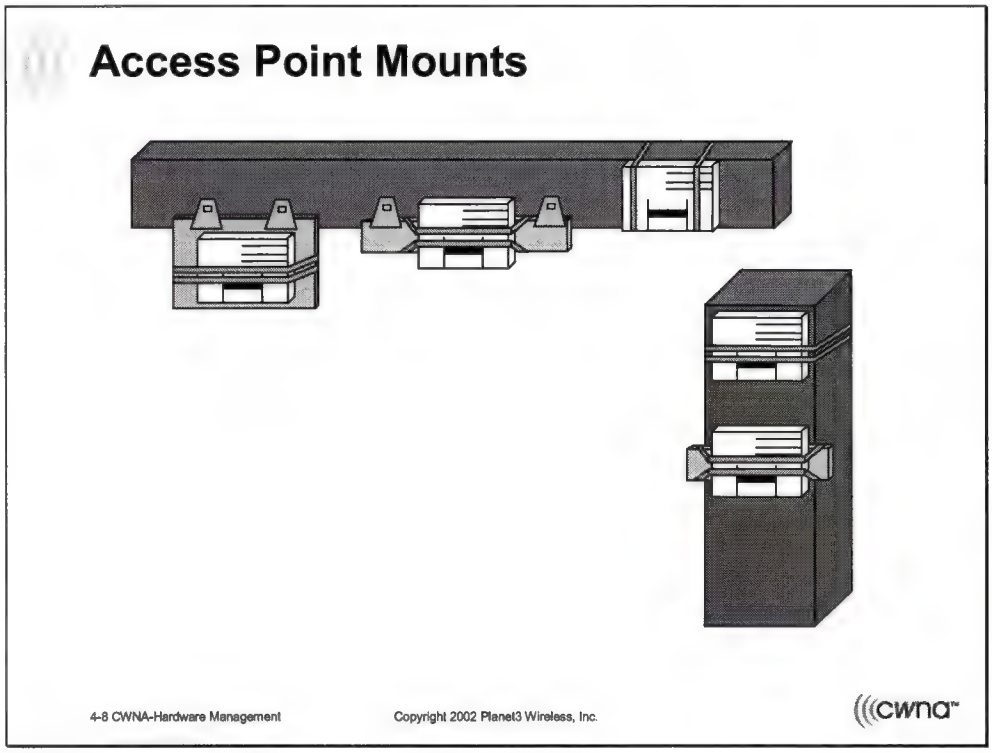
It is normal to see a minimum of 50% overlap of coverage between the repeater access point and the root access point when using omni-directional antennas (which is typically the case).

Copyright © 2003, Planet3 Wireless, Inc.



Bridge Mode

In bridge mode, access points serve as a bridge between two or more wired segments of the network. This configuration could be used to connect two office buildings that are next to each other but do not have wired connectivity to each other. Instead of incurring the cost of digging up the ground and laying cable between the buildings, or paying for an expensive T1 line, one access point is put in each building to connect the networks. This function is generally performed with a wireless bridge, but it is worth noting that some access points do have this functionality built in. It is sometimes simply a matter of configuration to convert an access point to a wireless bridge, depending on the manufacturer of the access point.

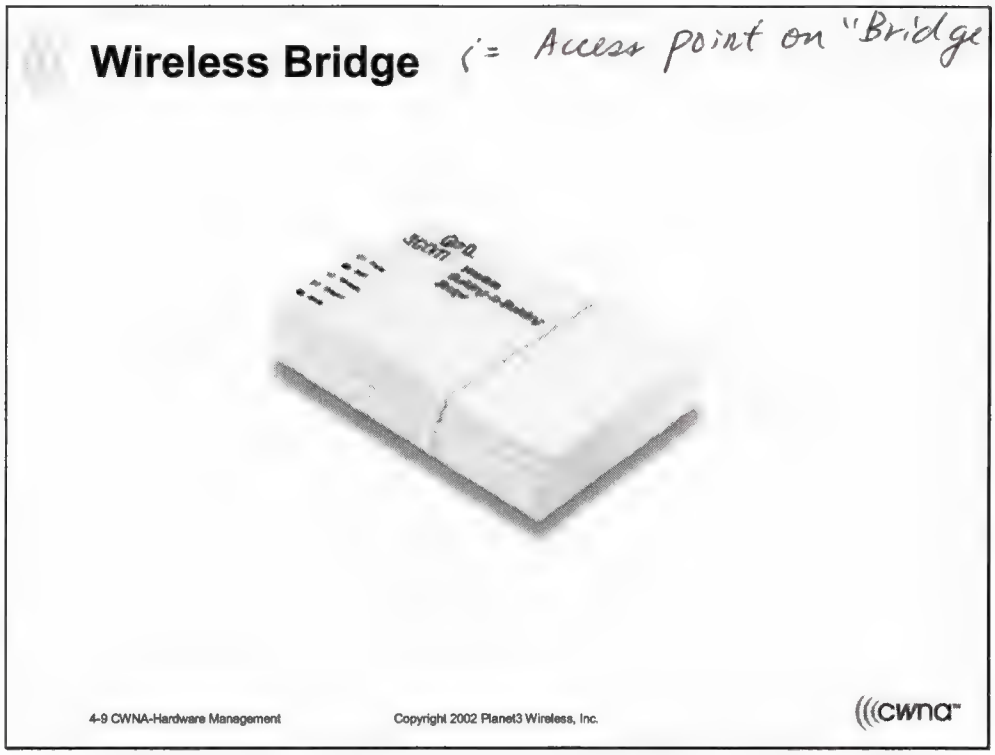


Access Point Mounts

Some things to keep in mind when mounting access points are:

- Use heavy duty zip ties to mount access points to columns or beams.
- Do not cover access point lights when mounting access point with zip ties.
- Mount access points upside down so that indicator lights can be seen from the floor
- Label access points
- When column mounting, it's possible to use a 2x4 beam as a base for the access point. Mount the 2x4 to the column and then mount the access point to the 2x4.
- When beam mounting, one may use zip ties directly or perhaps a 2x4 mounted to the beam with beam clamps with the access point mounted to it. Do not forget to mount the antenna the same way as is specified in the site survey
- Some access points come with slide mount holes and others may have a separate mounting kit or frame with which to mount them. Some do not, by design, allow for mounting.

Copyright © 2003, Planet3 Wireless, Inc.



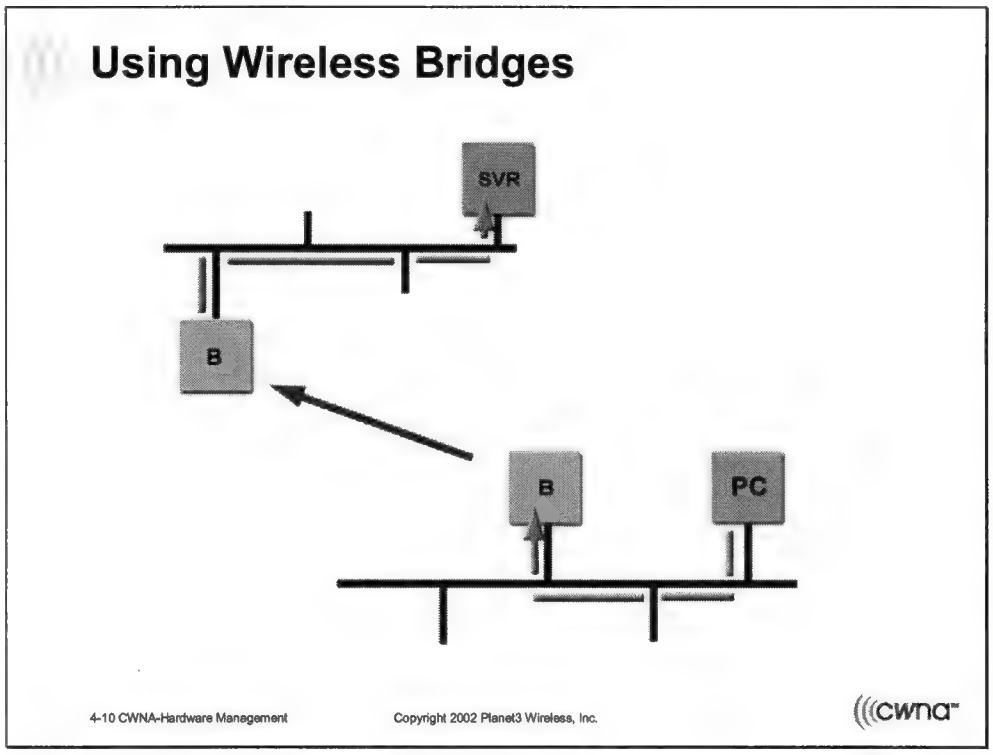
Wireless Bridge

A wireless bridge is a layer-2 device used to connect remote sites wirelessly to the main network. Wireless bridges can be used as repeaters to extend the range of the wireless segment. Wireless bridges are half-duplex devices capable of wireless connectivity in point-to-point or point-to-multipoint configurations. Wireless bridges are typically used in building-to-building connectivity.

Wireless Bridge Options

Options that may be found in wireless bridges may include:

- Fixed or detachable antennas (with or without diversity)
- Advanced filtering capabilities (MAC or Protocol)
- Removable (modular) radio cards
- Multiple radio capability
- Varied types of wired connectivity (10baseTx, 10/100baseTx, 100baseTx, 100baseFx, etc.)
- Some models can be configured to function as an access point or as an access point and bridge simultaneously.



Using Wireless Bridges

The illustration above shows how the wireless bridge functions to connect two wired segments of the network. The configuration is identical to when an access point is running in bridge mode. Two or more bridges can be in this type of configuration.

Setup and Installation

Wireless bridges can be managed and configured in many different ways. Some units may support terminal emulation sessions (telnet) while others may support web browser access (http). Some manufacturers offer custom configuration and management software. SNMP application support is featured in some models, and others may even have a legacy serial or USB port for access. It is important to choose a wireless bridge that is compatible with the network's management systems and methodology. Another important note about configuring wireless bridges is that most manufacturers include an application for helping align wireless bridges. This alignment application amounts to a signal strength meter that allows for optimizing the alignment and achieving the best throughput out of a wireless bridge link.

Copyright © 2003, Planet3 Wireless, Inc.

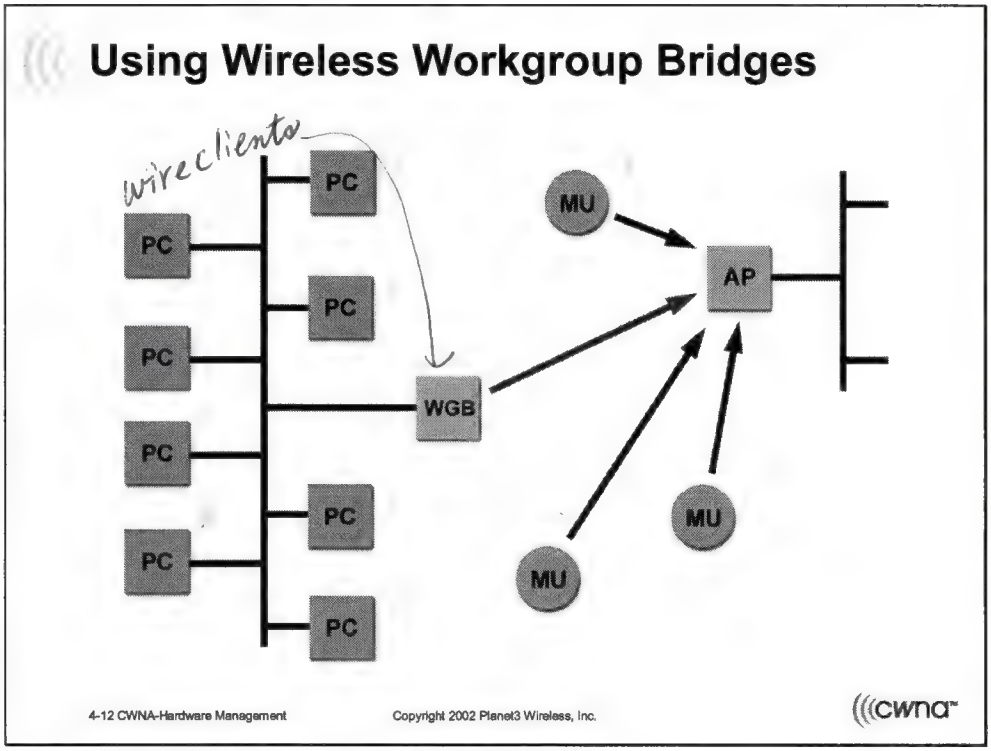
Wireless Workgroup Bridges

A wireless workgroup bridge (WGB) is used to connect a small group of wired users (normally 8 or less) from one wired network to another via a wireless link. The wireless workgroup bridge is a client device capable of aggregating the wired LAN users into a collective wireless LAN client. Users first connect to the wireless workgroup bridge through a standard Ethernet connection. Then the wireless workgroup bridge associates to an access point as a single client. This configuration allows the users behind the wireless workgroup bridge to access the other segment of the wired network as "collective client".

Wireless Workgroup Bridge Options

Options that may be found in wireless workgroup bridges may include:

- Fixed or detachable antennas (with or without diversity)
- Advanced filtering capabilities (MAC or Protocol)
- Variable output power
- Varied types of wired connectivity (10baseTx, 10/100baseTx, 100baseTx, 100baseFx, etc.)



Using Wireless Workgroup Bridges

As seen in the illustration above, an access point sees the wireless workgroup bridge as a single wireless LAN client device. In this case, there are eleven client computers that are accessing the network segment through the access point, but the access point is only aware of four clients. Eight of the clients are accessing the access point through the work group bridge.

Setup and Installation

Wireless workgroup bridges are typically configured through a web browser (http) or through terminal emulation (telnet) software. Some manufacturers implement a custom configuration application. Remember that wireless workgroup bridges are client devices on the wireless network and the management and configuration of these devices is usually less sophisticated than that of an access point or wireless bridge.

Copyright © 2003, Planet3 Wireless, Inc.

Wireless LAN Client Devices

Client Devices

Wireless LAN Client devices are configured in end-user stations that include:

- Desktops
- Laptops
- PDAs
- Handheld scanners

These are the types of devices that have the need for wireless connectivity into the network infrastructure.

PCMCIA & Compact Flash Cards

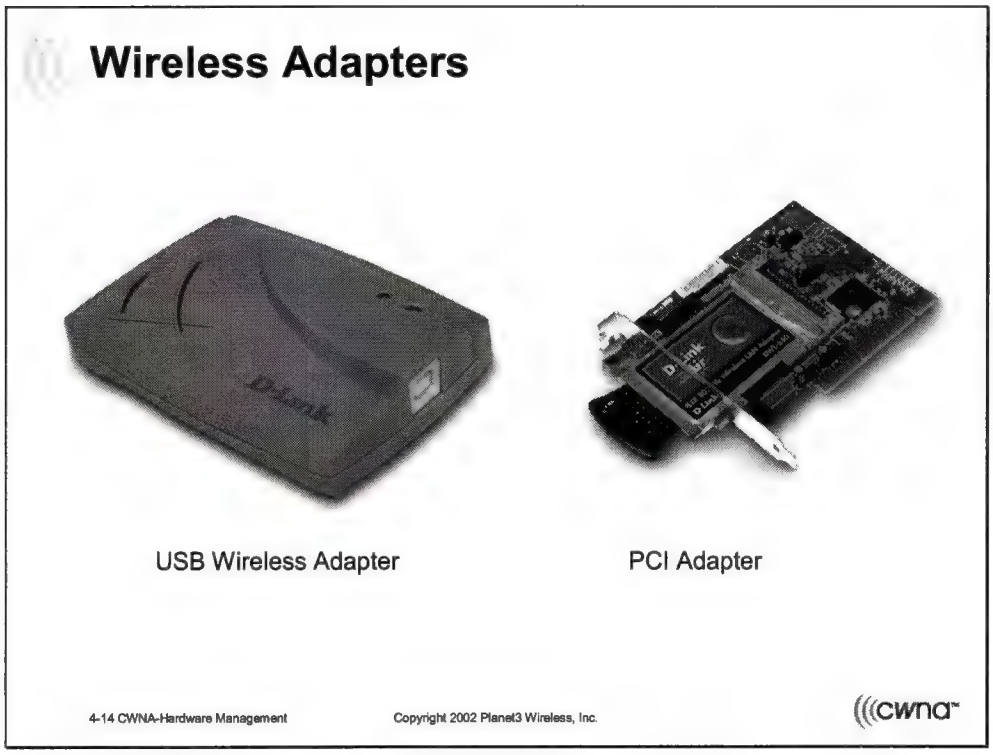
PCMCIA (PC Cards) and compact flash cards (CF Cards) are the most widely used type of client devices because they are used with notebooks, laptops, and PDA computers. Wireless cards can vary in their data rates, range, power output, and functionality options. Some models may include retractable, flexible, titanium wire antennas and others may include fixed, plastic-covered antennas. Because

antennas may get bumped or bent, the cards should be of a good quality to ensure they do not break easily. Antennas are easily broken, rendering the device useless.

Serial & Ethernet Converters

Serial and Ethernet converters are used with devices having legacy 9-pin serial ports or Ethernet ports, converting those connections into wireless LAN connections. Nine-pin serial devices are considered legacy devices, but can easily be found in industrial or manufacturing environments where older client computers exist. The converter devices that are currently available are often designed for plug-and-play installation to get up and running quickly.

Copyright © 2003, Planet3 Wireless, Inc.

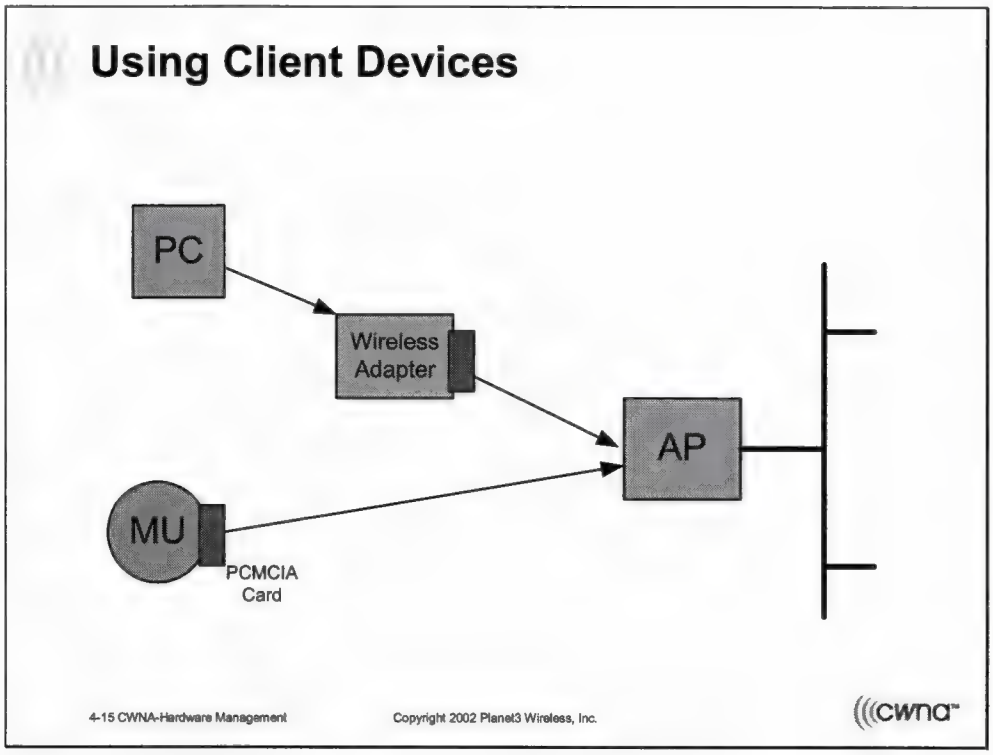


USB Devices

USB devices are used to provide wireless LAN connectivity through the USB port in a laptop, notebook, or desktop computer. Clients can connect to the wireless Ethernet network simply by plugging the USB client into a spare USB connector and loading the appropriate software. USB has the benefit of not requiring a bus card installation, changing IRQs, or searching for ISA or PCI slots. Most USB wireless client devices have a built-in power supply, and USB devices are generally less expensive than PCI or ISA cards. Some USB units do not come with an integrated wireless LAN radio card. In this case, the USB device is considered to be a USB adapter. This adapter will accept a wireless LAN PC Card in a PCMCIA slot. When this is the case, the user typically has to load drivers for the adapter and the radio card then load the utility software for the radio card.

PCI/ISA Devices

PCI and ISA cards are used inside desktop or server computers. ISA cards are considered legacy and require manual configuration. PCI cards generally support Plug-and-Play, which makes setup relatively easy. PCI Adapters are PCI cards that accept PCMCIA cards for wireless connectivity. The adapters themselves are inexpensive but require the purchase of a PCMCIA card in order to get wireless connectivity. For users who may have both a laptop and a desktop, a PCMCIA card could be shared between the two computers as long as only one computer needs network access at a time.



Using Client Devices

Setup and Installation

There are two parts to installing wireless LAN client devices.

1. Installing the Drivers

Software drivers are provided for client devices so the computer they will be running on can recognize and use the device. When selecting a client device for a computer, make sure the manufacturer includes drivers for the specific operating system being used.

Serial and Ethernet converters require no special drivers to function but do require configuration which is typically handled through custom software provided by the manufacturer.

2. Installing Manufacturer-specific Utilities

Manufacturers supply utilities for configuring client devices to ensure optimal connectivity and throughput. Depending on the manufacturer, the client software may also include some of the following utilities:

- Site Survey tools
- Spectrum Analyzer

Copyright © 2003, Planet3 Wireless, Inc.

- Power & Speed monitoring tools

Manufacturer Utilities

Manufacturers' utilities vary greatly in functionality, but share a common set of configurable parameters:

- Infrastructure/Ad Hoc mode
- SSID (Network Name)
- Channel (if in Ad Hoc mode)
- WEP Keys
- Authentication Type (Open System, Shared Key)

Copyright © 2003, Planet3 Wireless, Inc.

Gateways

Wireless Residential Gateway

A Wireless residential gateway is a device designed to connect a small number of wireless nodes (25 or fewer) to a single device for Layer 2 or Layer 3 connectivity to the Internet or another network. These units have a built-in access point. They are typically used in a SOHO environment to connect users to the Internet via:

- Analog modem
- xDSL
- Cable modem
- Satellite modem

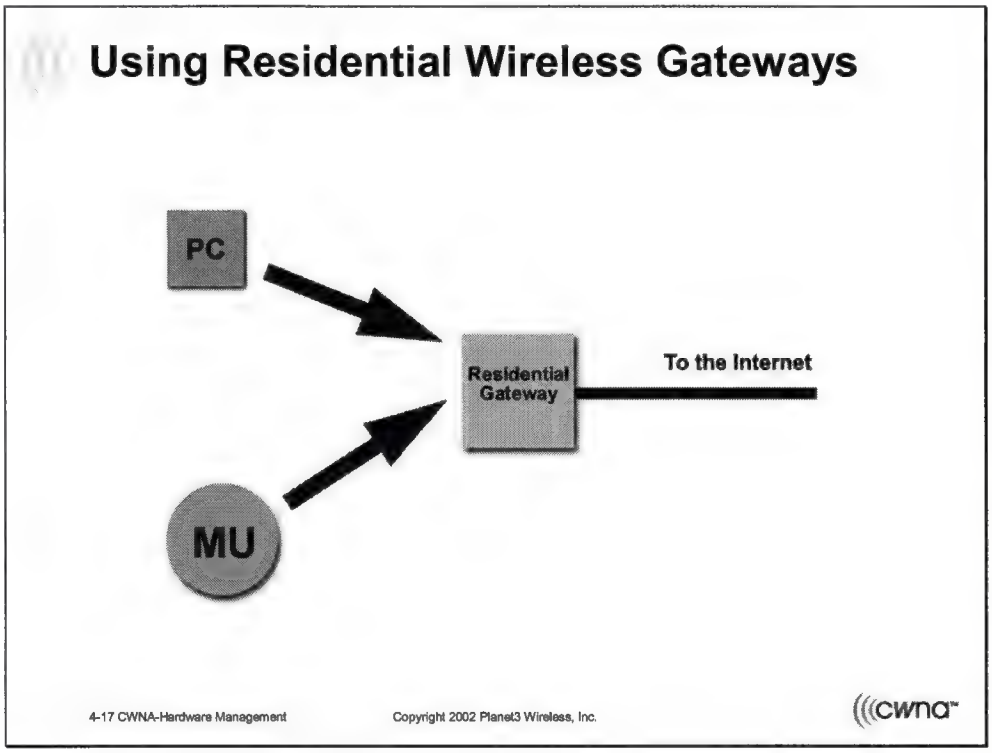
The wireless residential gateway is an ideal solution for homes where multiple computers are present that need to connect to the Internet at the same time. Wireless network adapters installed in each client receive the data from the gateway.

Wireless residential gateways can include options for:

- PPPoE
- NAT
- Internal hub or switch
- Firewall

Copyright © 2003, Planet3 Wireless, Inc.

- DHCP server & client
- Access point
- Backup serial connectivity
- Virtual servers
- Print server

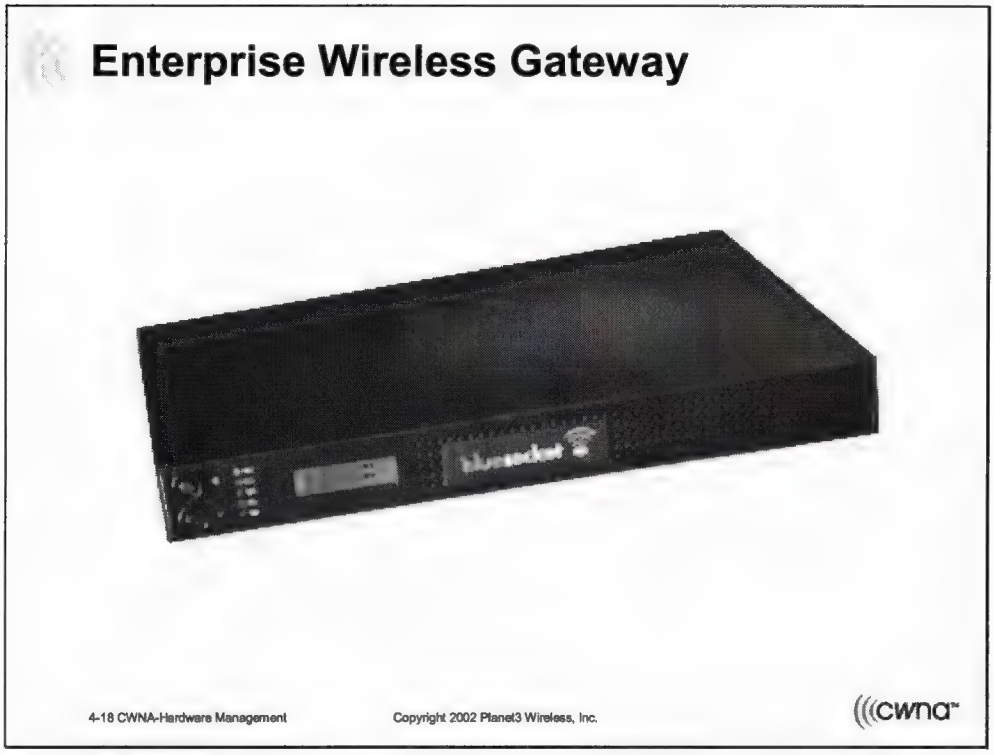


Using Wireless Residential Gateways

Setup and Installation

Configuring and installing wireless residential gateways usually consists of browsing to the built-in HTTP server via the Ethernet port and changing the user-configurable settings to meet the particular needs of the network. Some units have only console or telnet text-menu access available, which makes configuration a little less user-friendly. Managing the gateway normally consists of browsing to the built-in HTTP server to change settings or to monitor items such as up-time or dynamic IP addresses. These devices serve as an all-in-one connectivity device for the home or small office. Prices of these devices are very competitive, and most offer many features.

Copyright © 2003, Planet3 Wireless, Inc.

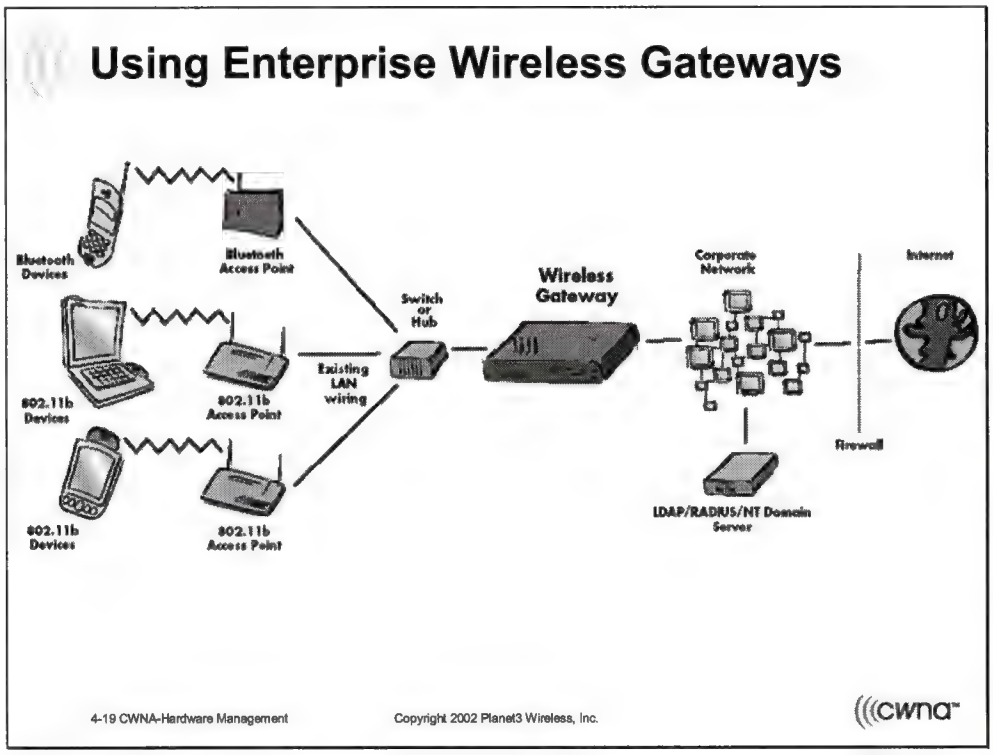


Enterprise Wireless Gateways

An enterprise wireless gateway is a device that provides VPN connectivity and backend authentication methods for wireless access on a network. These devices are appropriate for large-scale wireless LAN environments providing a multitude of manageable wireless LAN services such as rate limiting and Quality of Service (QoS). QoS is defined as the ability to control the capacity each user gets so one user is unable to saturate the entire 11Mbps capacity of the network. Features that may be found in an enterprise wireless gateway may include RADIUS support, IPSec with certificates, PPTP/L2TP protocol support, a broad range of wireless LAN standards support, and a wide range of management support.

Enterprise wireless gateways support special protocols for wireless but they are not wireless devices. These units are situated between the access points and the wired network. Wireless gateways, although expensive, offer much functionality and can support many access points. 100 Mbps wired Ethernet connectivity, hot fail-over support, and powerful processing make wireless gateways a valuable asset in any wireless LAN environment.

Some vendors have built in 'profile' management where different profiles can be setup for groups or types of users. This is sometimes referred to as role-based access control (RBAC). In large-scale installations where there are many mobile units, users may have different privileges and access to network resources depending on their location or their user category.



Using Enterprise Wireless Gateways

Setup and Installation

Enterprise wireless gateways are generally installed in the signal path on the wired LAN segment between the access point and the upstream hub or switch.

Configuration of the units is done through console ports, telnet, or internal HTTP servers. SNMP support is generally included to allow enterprise wide simultaneous upgrading of access points via “profiles”. In some units, Master/Slave functionality is configurable. This type of functionality allows for a single "master" wireless gateway to be configured, and the configuration changes pushed to its "slave" units. This functionality helps reduce administration time of the network.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

5 Antennas and Accessories

Objectives

Upon completion of this chapter you will be able to:

- Explain the types of wireless LAN antennas and how/when to use them
- Describe the various wireless LAN accessories and where they are used

5-2 CWNA-Antennas and Accessories

Copyright 2002 Planet3 Wireless, Inc.

Chapter Content

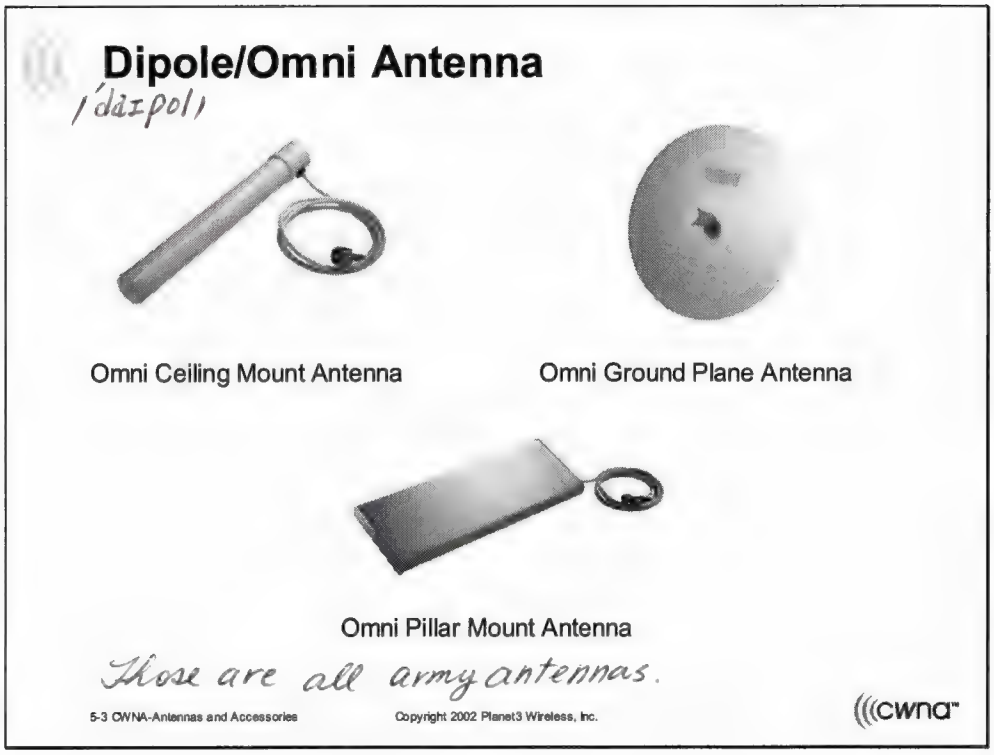
There are three general categories into which all wireless LAN antennas fall: omnidirectional, semi-directional, and directional. The attributes of each of these groups will be discussed in depth, as well as the proper methods for installing each kind of antenna. Also explained are the many different hardware devices that are used to connect antennas to other wireless LAN hardware.

The chapter outline follows:

- RF Antennas
- Power over Ethernet Devices
- Accessories

Copyright © 2003, Planet3 Wireless, Inc.

RF Antennas



Overview

An RF Antenna is a device used to convert high frequency (RF) signals on a transmission line (a cable or waveguide) into propagated waves in the air.

The electrical fields emitted from antennas are called *beams* or *lobes*.

Dipole/Omni-directional

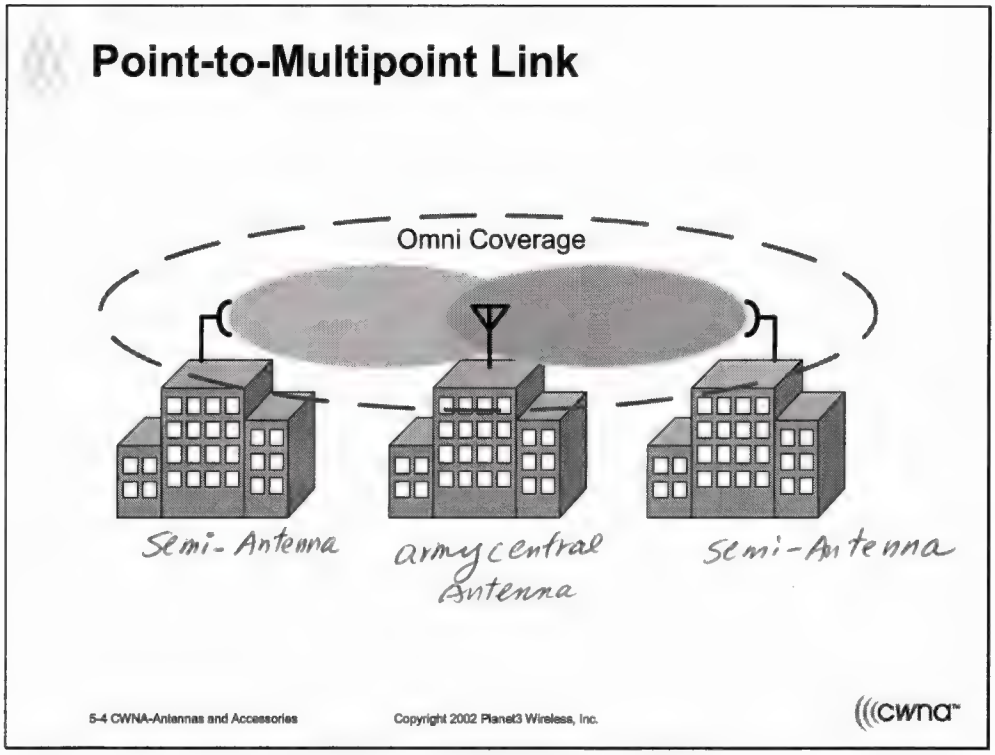
Omni-directional (OMNI) or dipole antennas produce a 360-degree horizontal beam resembling a doughnut. These types of antennas are most effective with a hub-n-spoke topology that is common in local area and wide area networks. When used outdoors, omni antennas are usually used in a center location such as a building in the center of a campus. Using the antenna in this fashion where it is located in the middle of the desired coverage area yields the greatest coverage area. When used indoors, omni antennas are typically located in a central area such as a hallway or in the middle of a large room.

In a high-gain omni antenna, the beam is squeezed vertically to reach further horizontal destinations.

Copyright © 2003, Planet3 Wireless, Inc.

Consider a tradeshow, where often there will be wireless network capabilities on the show floor. These tradeshow facilities may have ceilings that are 40 feet high. Placing an access point with a high-gain omni antenna in the ceiling will not provide the best coverage because all of the users are on the show floor. With a low gain omni-directional antenna placed in the ceiling, the doughnut-shaped coverage area is not squeezed, so the likelihood of coverage near the floor is good. Depending on interfering obstacles, it might be a good solution to place a high-gain omni antenna near the floor in order to provide adequate coverage for these users at great distances from the access point.

Copyright © 2003, Planet3 Wireless, Inc.

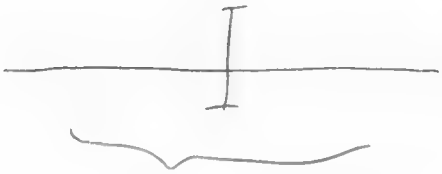


Point-to-Multipoint Link

This diagram illustrates the hub-n-spoke type of topology commonly used with omni-directional antennas. The omni antenna is placed in a central location, in this case the building in the middle of the coverage area. The coverage area of the antenna reaches both of the other buildings on either side of the central building.

Semi- Antenna

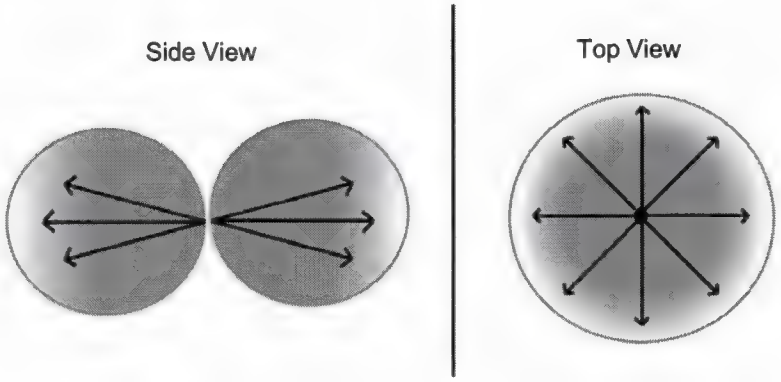
- less interference
- small coverage
- can concentrate more



more horizontal (broad)
less vertical ( )

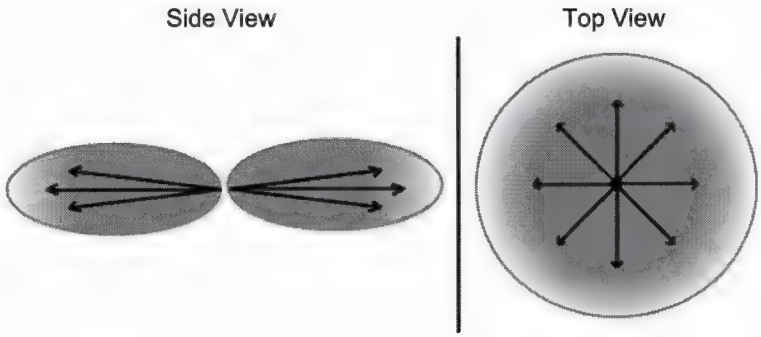
Omni-directional Antenna Radiation Pattern

omni



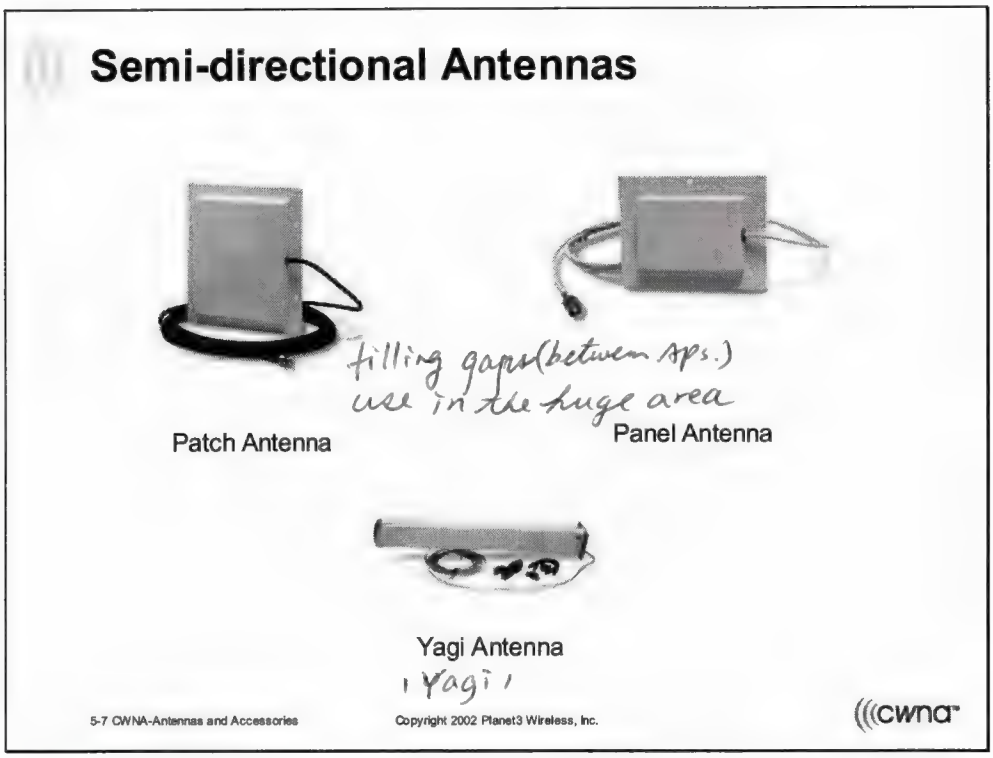
Copyright 2002 Planet3 Wireless, Inc.

High-Gain Omni-directional Antenna Radiation Pattern



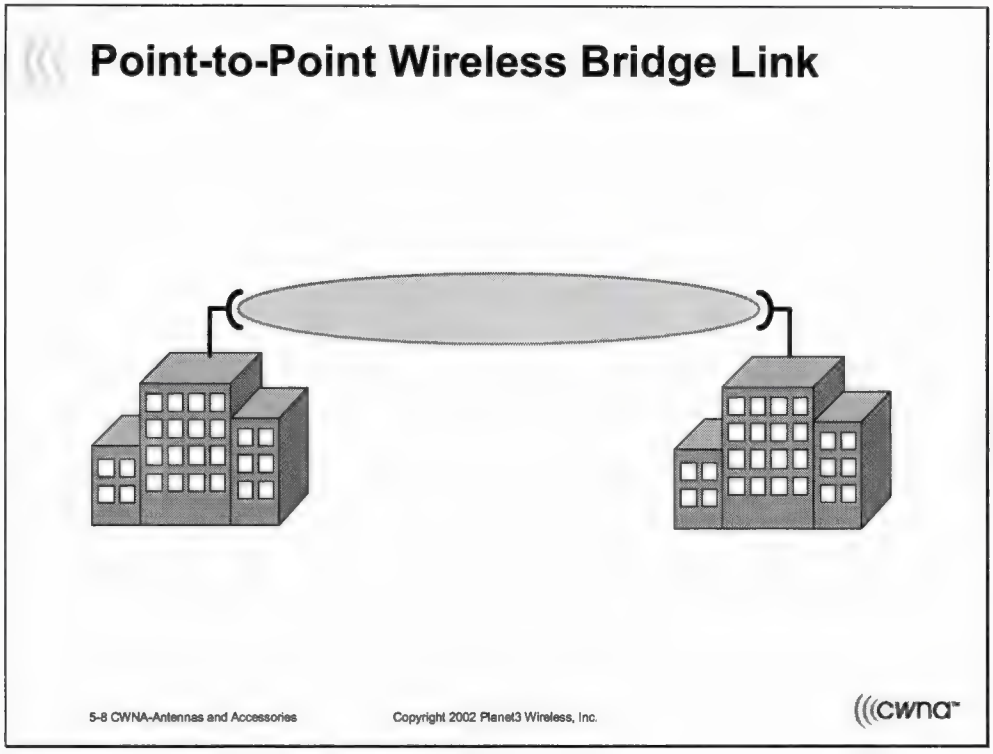
Copyright 2002 Planet3 Wireless, Inc.

Copyright © 2003, Planet3 Wireless, Inc.



Semi-Directional Antennas

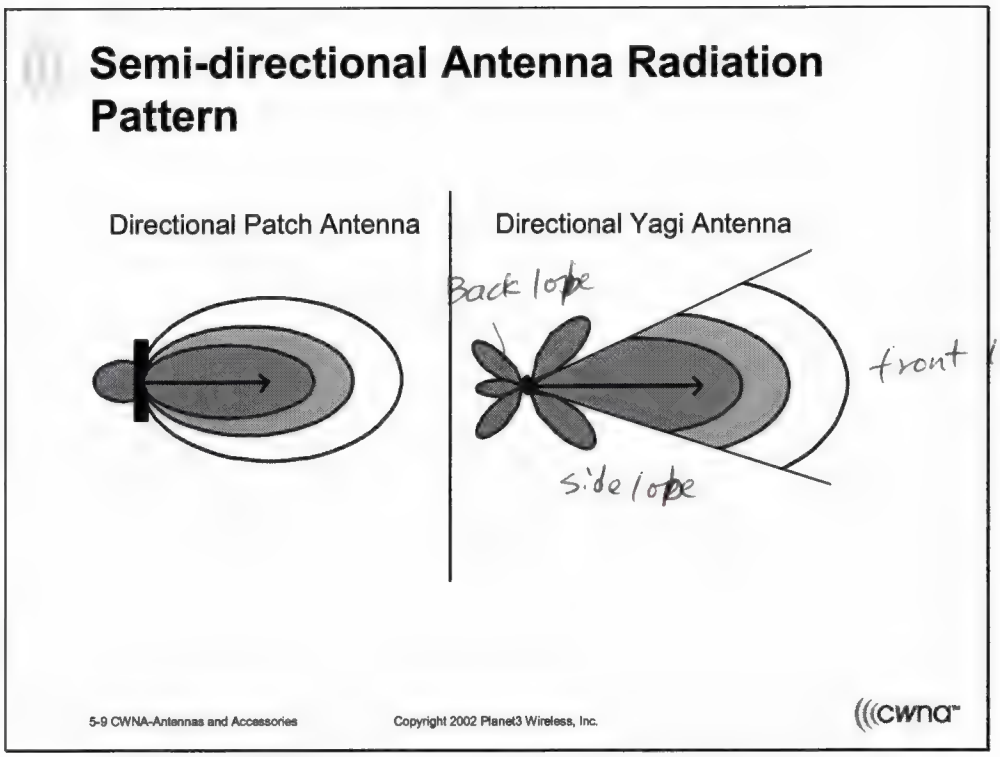
The patch, panel, and Yagi antennas are types of semi-directional antennas. Each of the different varieties has a different radiation pattern. These antennas are flat in design so that they can be mounted on walls or other flat surfaces. A semi-directional antenna has a back lobe and side lobes that should be taken into consideration when configuring wireless LANs. The radiation pattern results in a hemispherical or cylindrical coverage area. This type of antenna is ideal for short to medium range bridging and for access point coverage down long hallways or corridors.



Point-to-Point Wireless Bridge Link

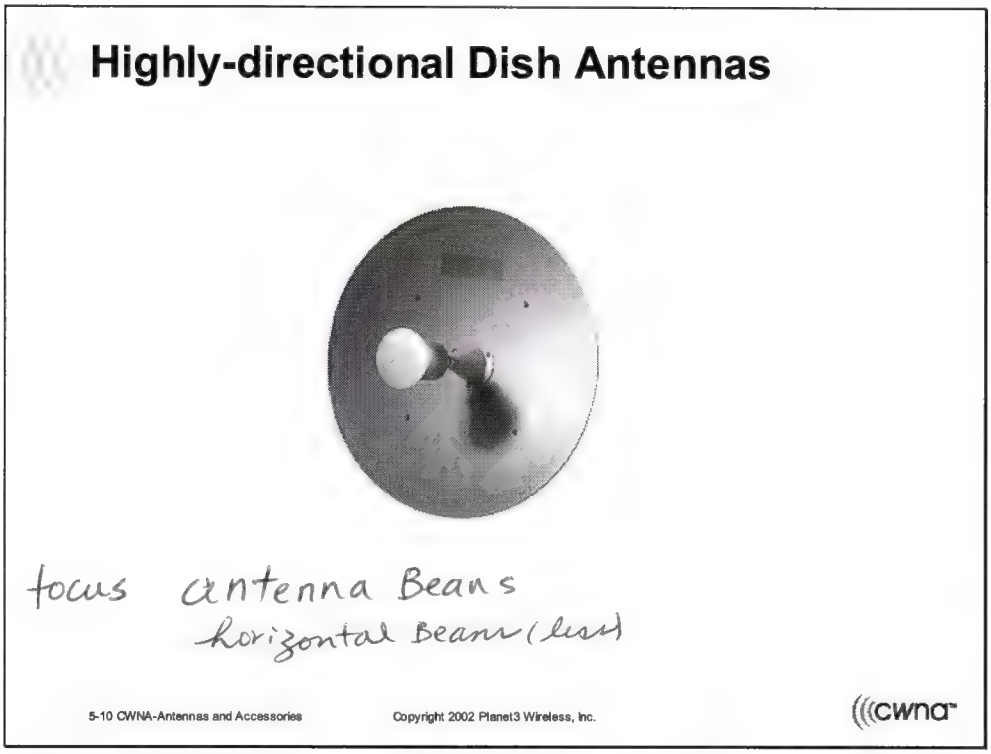
A point-to-point wireless bridge link usually uses some type of semi-directional antenna. This type of signal radiation helps with security because there is not as great a worry about other people intercepting the signal. In this scenario, attention needs to be paid to making sure that the strength of the signal is not so great that the signal could be intercepted by having the signal transmit past the receiving building.

Copyright © 2003, Planet3 Wireless, Inc.



Semi-directional Antenna Radiation Patterns

Semi-directional antennas have several lobes, each useable in a wireless LAN. While the forward (front) lobe is the largest and most pronounced, using the back (rear) lobe and the side lobes is quite common in good wireless LAN installations. Depending on the antenna type, the side and rear lobes can be quite large or even non-existent. A good wireless LAN installation makes use of as many of the lobes of the semi-directional antennas as possible. Semi-directional antennas have extended forward reach due to having given up gain in other areas. This extended reach is part of the antenna's design.



Highly-directional Antenna

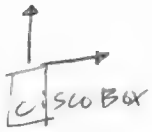
Highly-directional antennas are concave in appearance, and are typically called parabolic dishes. Highly-directional antennas are similar in appearance to a satellite dish with the same concave shape, although they are much smaller in size than a typical satellite dish. These antennas have the highest available gain of all the wireless LAN-compatible antenna types, and the narrowest beamwidth. Highly-directional antennas are ideal for point-to-point links that cover long distances.

Copyright © 2003, Planet3 Wireless, Inc.

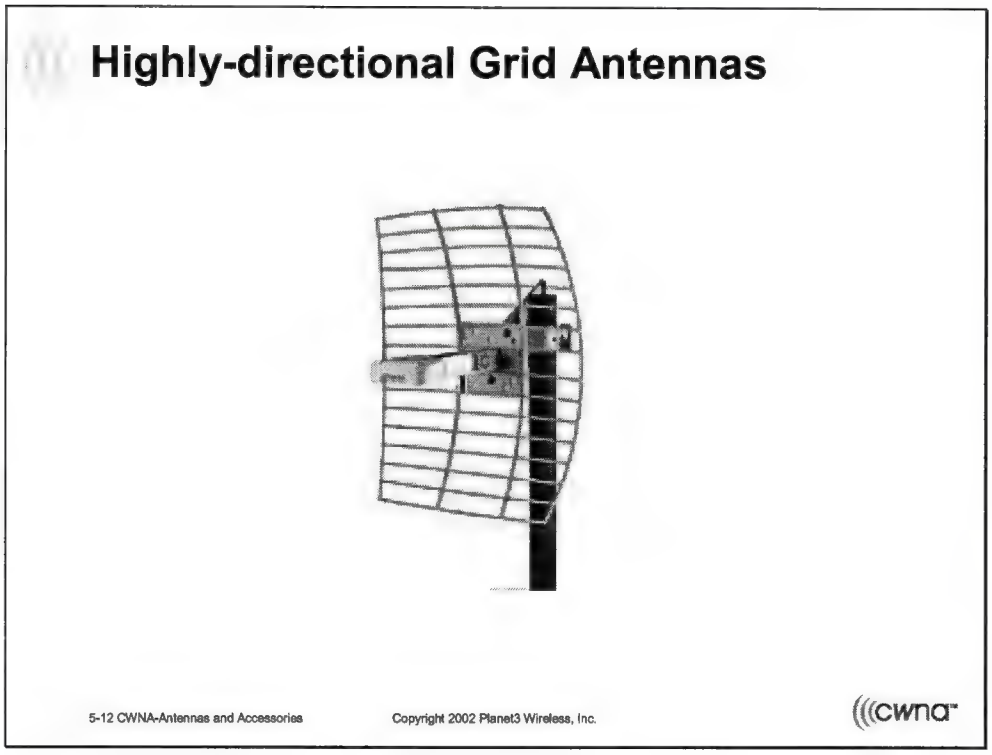
Highly-directional Dish Antenna Radiation Pattern

5-11 CWNA-Antennas and Accessories Copyright 2002 Planet3 Wireless, Inc. ((cwna™

Note In a highly-directional antenna, where the beamwidths are only 4-5 degrees wide, wind can cause the signal to be cut-off if it moves the antenna around even slightly. It is important to fasten the antenna very securely to the mount to make sure it does not move. The mount must be securely fastened to the tower, pole, wall, or other surface as well.

antenna inversity :  don't do this.

Copyright © 2003, Planet3 Wireless, Inc.



Grid Antenna

Grid antennas are highly-directional antennas, and they use a parabolic reflector to focus the RF energy. Instead of a dish, a grid antenna uses a metal grid as a reflector. The grid may be circular or rectangular in shape, and constructed from formed metal wire, tubing, or bar stock; or it may be cast from aluminum or other metal.

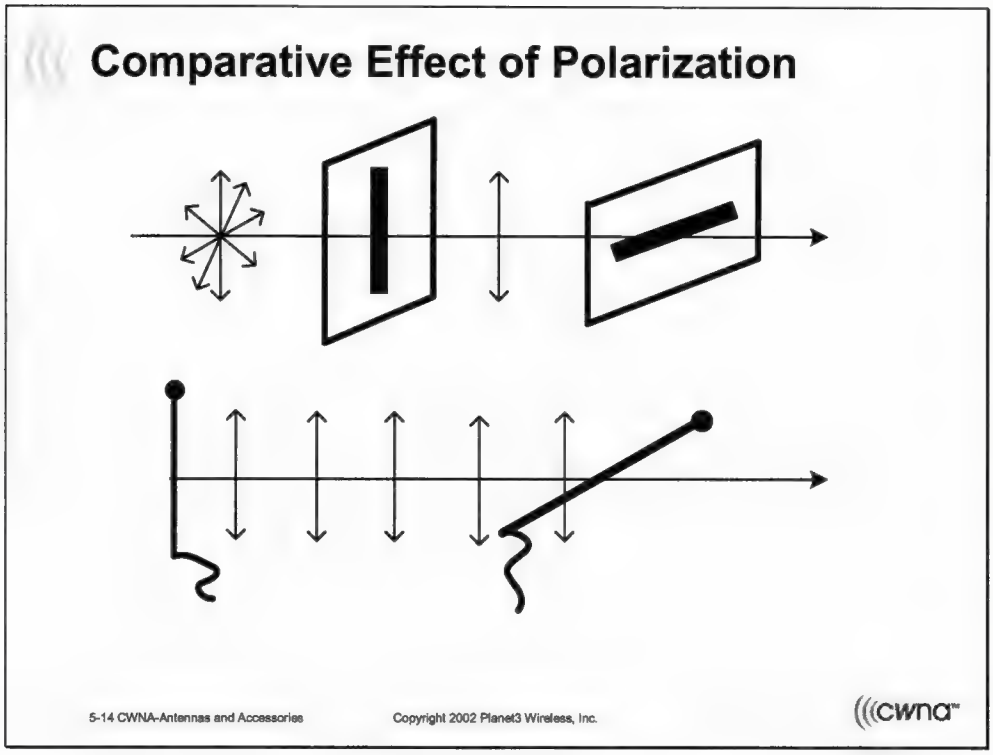
While the beam width is not quite as narrow and the gain not quite as large as a highly-directional dish antenna, the grid antenna is superior in its wind loading characteristics. Most of the grid's reflector area is open, allowing for the wind to flow through it. This allows the grid antenna to withstand significantly higher winds than a dish antenna. Grid antennas are excellent for outdoor point-to-point links that cover long distances.

Copyright © 2003, Planet3 Wireless, Inc.

Highly-directional Grid Antenna Radiation Pattern

5-13 CWNA-Antennas and Accessories Copyright 2002 Planet3 Wireless, Inc. cwna

Note A grid antenna, where the beamwidths are only 5-10 degrees wide, wind can cause the signal to be cut-off if it moves the antenna around even slightly. Grid antennas can withstand much stronger winds than their highly-directional dish counterparts. It is always important to fasten the antenna very securely to the mount to make sure it does not move. The mount must be securely fastened to the tower, pole, wall, or other surface as well.



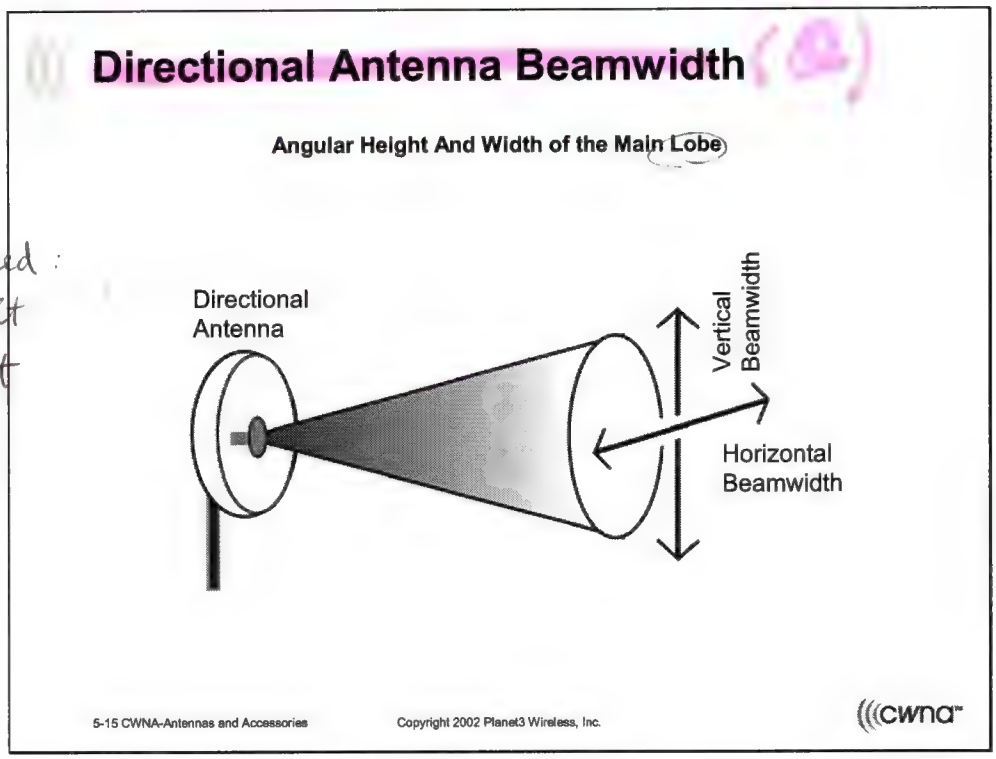
Polarization

Antenna polarization is the physical orientation of the antenna along a horizontal or vertical plane. Because antennas that are not polarized the same way cannot communicate with each other, it is important to know the effects of polarization.

Vertical polarization is when the antenna is oriented such that it has a perpendicular plane to the Earth. This is the type of polarization most often used in wireless LANs.

Horizontal polarization is when the antenna is oriented such that it has a parallel plane to the Earth. This type of polarization is typically used for broadcasting.

Copyright © 2003, Planet3 Wireless, Inc.



system can be changed: receiving on the right transmitting ... left

Antenna Gain and Beamwidth

Antenna gain is a measure of how much the RF input power is concentrated in a particular direction as it is propagated from the antenna. The gain of an antenna is measured in dBi, which is a measure of decibels referenced to an isotropic radiator. Narrowing (focusing) the beams (lobes) increases antenna gain.

An antenna's beamwidth is a measure of the angle between the two half-power (-3 dB) points on either side of the main lobe when referenced to the peak effective radiated power of the main lobe. A 6 dBi gain equates to doubling the radiated distance.

Vertical beamwidth is measured in degrees perpendicular to the Earth's surface.

Horizontal beamwidth is measured in degrees parallel to the Earth's surface.

Free-Space Path Loss

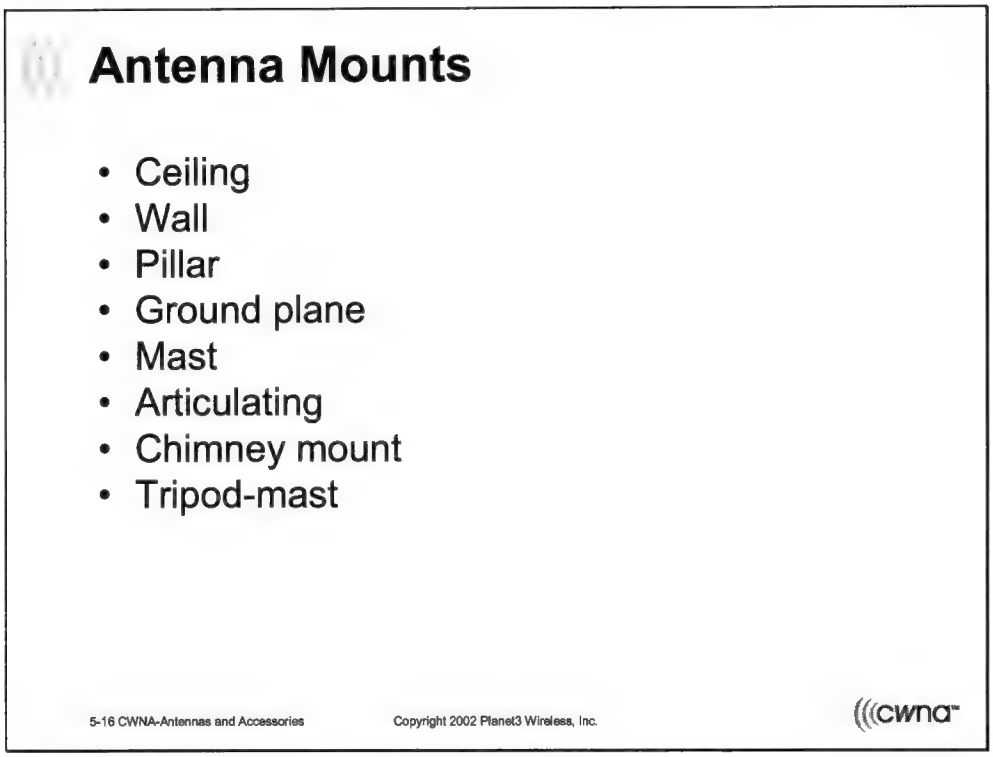
Free-Space Path Loss (often called just path loss) is a reference to the loss incurred by an RF signal due largely to "signal dispersion" which is a natural broadening of the wave front. The wider the wave front, the less power can be induced into the receiving antenna. Free-Space Path Loss describes this loss of signal strength as a function of distance alone and becomes a very important factor when considering link viability. An important thing to consider here is that wireless LAN antennas have a small receiving surface area, which also plays into Path Loss. The further

the transmission path and the smaller the receiving aperture, the greater the path loss will be.

Common Antenna Beamwidths

Antenna Type	Horizontal Beamwidth (in degrees)	Vertical Beamwidth (in degrees)
Omni-directional	360	Ranges from 7-80
Patch/Panel	Ranges from 30-180	Ranges from 6-90
Yagi	Ranges from 30-78	Ranges from 14-64
Parabolic Dish	Ranges from 4.6-25	Ranges from 4.6-21

Copyright © 2003, Planet3 Wireless, Inc.

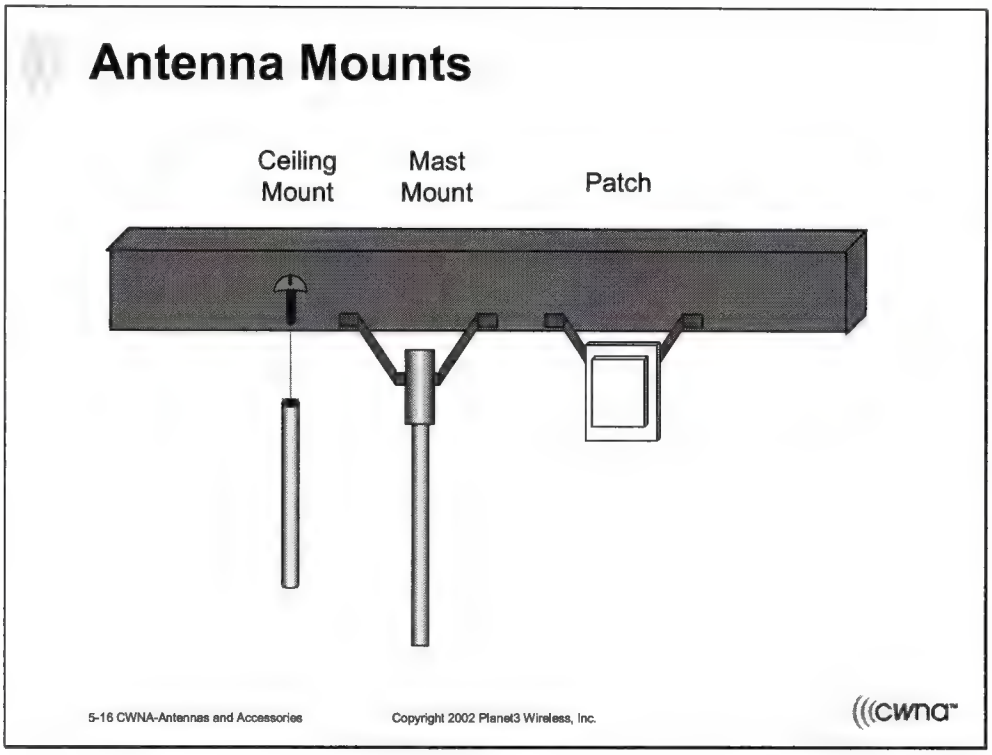


Antenna Mounts

There are many ways to mount an antenna depending on what type of antenna is being used. Each method poses its own challenges and may call for special mounting hardware.

- Ceiling – typically hung from crossbars or drop ceilings
- Wall – forces the antenna away from a perpendicular surface
- Pillar – the antenna mounts flush to a perpendicular surface
- Ground plane – the antenna sits flatly on the ground
- Mast – the antenna mounts to a pole
- Articulating – a movable mast mount
- Chimney mount – includes various hardware to allow an antenna to be mounted to a chimney
- Tripod-mast – the antenna sits on top of a tripod

Copyright © 2003, Planet3 Wireless, Inc.



Some things to keep in mind when mounting antennas are:

- Many times the brackets shipped with the antenna may not work for a particular situation. Modifying brackets or building custom brackets may be necessary.
- Do not hang an antenna by its cable and make sure the mounting is solid and secure. The cable can break and cable sway can produce a moving cell.
- Exactly how the antenna is to be mounting should be specified for each antenna in the site survey report.

Copyright © 2003, Planet3 Wireless, Inc.

data/signal lost on the connector

"Buy tapes" to protect the connectors.
tape-y (electronic tapes)
22.29 compone pasta

RF Antenna Installation/Configuration

- Proper orientation
- Precise alignment
- Secure mounting
- Avoid conductive areas
- Prevent moisture
- Avoid obstructions
- Best coverage

5-18 CWNA-Antennas and Accessories Copyright 2002 Planet3 Wireless, Inc. ((cwna™

RF Antenna Installation and Configuration

To get the best throughput and coverage, and most longevity from antenna equipment, the following are suggested when installing and configuring the RF antennas mentioned in this chapter.

Proper Orientation

It is important to orient the antenna properly. Antennas used at two ends of a point-to-point bridge link, for example, should both be oriented in the same fashion – either horizontal or vertical. Due to polarization effects, not orienting the antennas correctly will result in little to no signal being received.

Precise Alignment

Antennas should be precisely aligned for optimum throughput. Bridge link utility software, provided by the wireless LAN bridge manufacturer, can be used to help optimize alignment. Optimized alignment will minimize:

- Lost packets
- High retry counts
- Low signal strength

Secure Mounting

Antennas should be secured properly so that wind does not move the antennas, which could negatively affect the signal. Antennas should not move from the position in which they were placed for the best signal reception. Using the proper mounting hardware when securing the antenna will reduce the chance of antenna movement.

Avoid Conductive Areas

A direct lightning strike to an antenna will destroy the unit and other parts of the wireless LAN that are along the same signal path. If lightning is a common problem, the antenna should be placed in a location not conductive to direct lightning strikes. Lightning rods should be placed somewhat nearby (but still at a reasonable distance) with very good Earth grounds so that lightning is directed away from the wireless LAN antenna.

Prevent Moisture

Moisture that enters into the antenna cables or connectors will cause damage to the devices and can affect RF signals. To prevent moisture entry into antenna cables, seal all external cable connectors using commercial grade sealers such as electrical tape and Coax-Seal.

Avoid Obstructions

When installing an antenna outdoors, obstructions such as trees or buildings that may interfere with the signal path should be avoided. Obstructions will reduce the amount of signal that is received, reducing the throughput of the connection. It is also important to consider anything that may become a future obstruction, such as any construction that is going on in the area.

Best Coverage

When using an omni-directional antenna, the device should be mounted in the center of the desired coverage area whenever possible. Using this hub and spoke approach ensures the maximum number of users can be reached.

Antennas should be placed as high as possible to increase the coverage area and to decrease the chance of obstructions. For example, an antenna that is placed on top of a cubicle will not have as good as coverage as one that is ceiling mounted. However an antenna that is mounted too high can also have poor coverage.

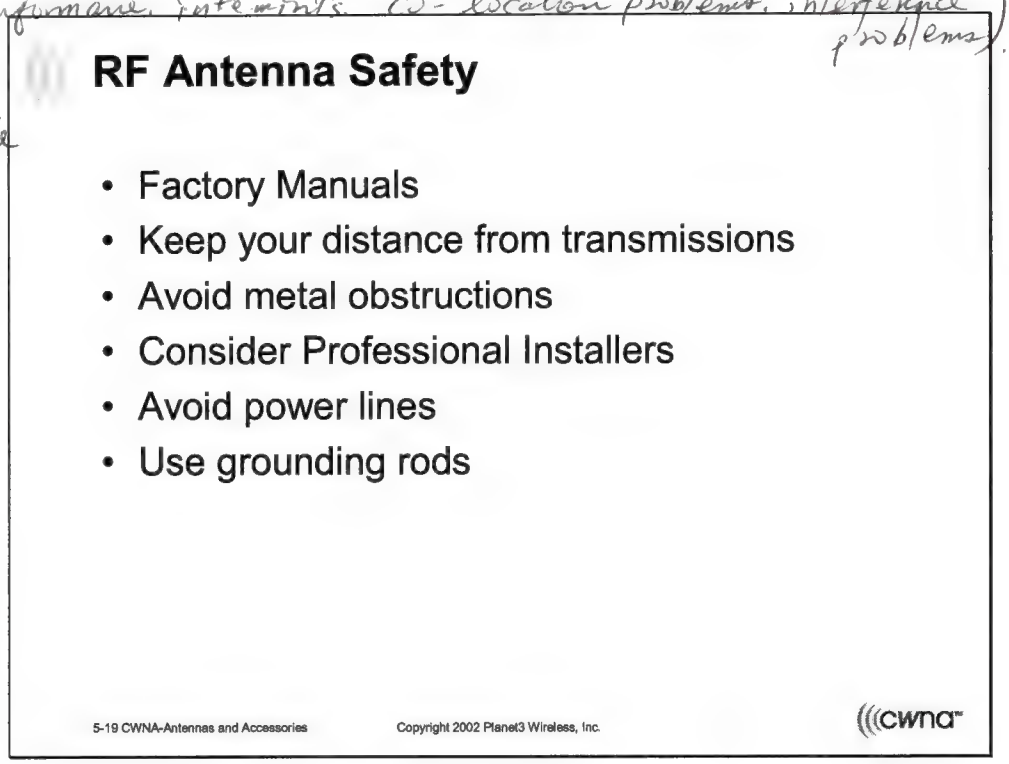
For best results, indoor antennas should only be used indoors and outdoor antennas should only be used outdoors. In the case where an indoor area is very large, such as a very large warehouse, an outdoor antenna can be used.

Copyright © 2003, Planet3 Wireless, Inc.

- signal strength lose
- errors Rate (retry the packets
- complains (port performance, interments, co-location problems, interference problems).

especially:
something at outside

Drip loop happened:



RF Antenna Safety

Installing antennas can sometimes be dangerous and can result in personal injury or damage to the antennas themselves. The following guidelines are some of the precautions to take to ensure a safe installation.

Factory Manuals

Carefully follow all instructions provided with an antenna. The manufacturer will include details on the installation and what the proper installation steps are.

Stay Away from Transmissions

Never touch a high-gain antenna to any part of the body or point it towards the body while it is transmitting. High-gain antennas can have the equivalent power output of a microwave oven in a very focused beam, and can result in serious internal injuries.

Avoid Metal Obstructions

Keep antennas away from metal obstructions such as:

- Heating and air-conditioning ducts
- Large ceiling trusses
- Building superstructures
- Major power cabling runs

These objects can cause the signal of the antenna to reflect off of the surface of the object. In the case of a high-gain antenna with high-power output, this redirection of the signal can cause injury to people or items in the way of the reflected path. This situation is rare due to path loss, but under certain circumstances, it is possible.

Consider Professional Installers

For most elevated antenna installations, consider using a professional installer to mount the unit. Professional installers have the correct equipment and experience to mount antennas in hard-to-reach areas such as towers or on the top or sides of tall buildings. The cost incurred for the service of a professional installer is small considering the installation will be done correctly with a reduced risk of injury.

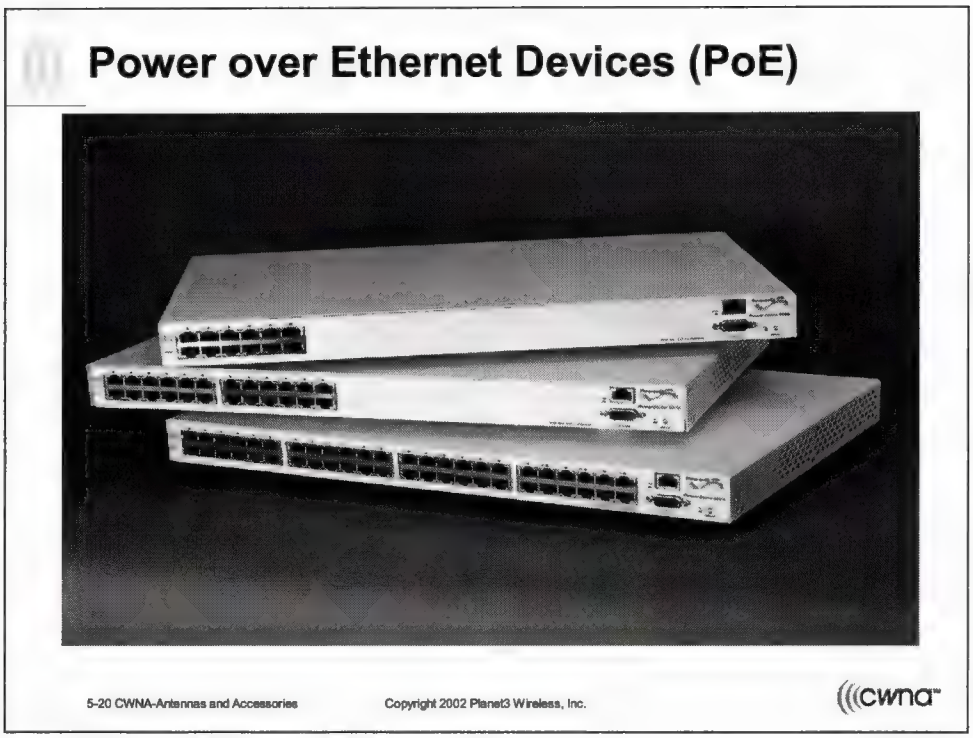
Avoid Power Lines

Antennas should be installed a safe distance from overhead power lines. The recommended distance is twice the antenna-mounted height.

Use Grounding Rods

Use special grounding rods and follow the National Electrical Code (NEC) or local electrical codes for proper outdoor antenna and tower grounding. Proper grounding will help protect equipment from transient electrical current from lightning strikes.

Copyright © 2003, Planet3 Wireless, Inc.

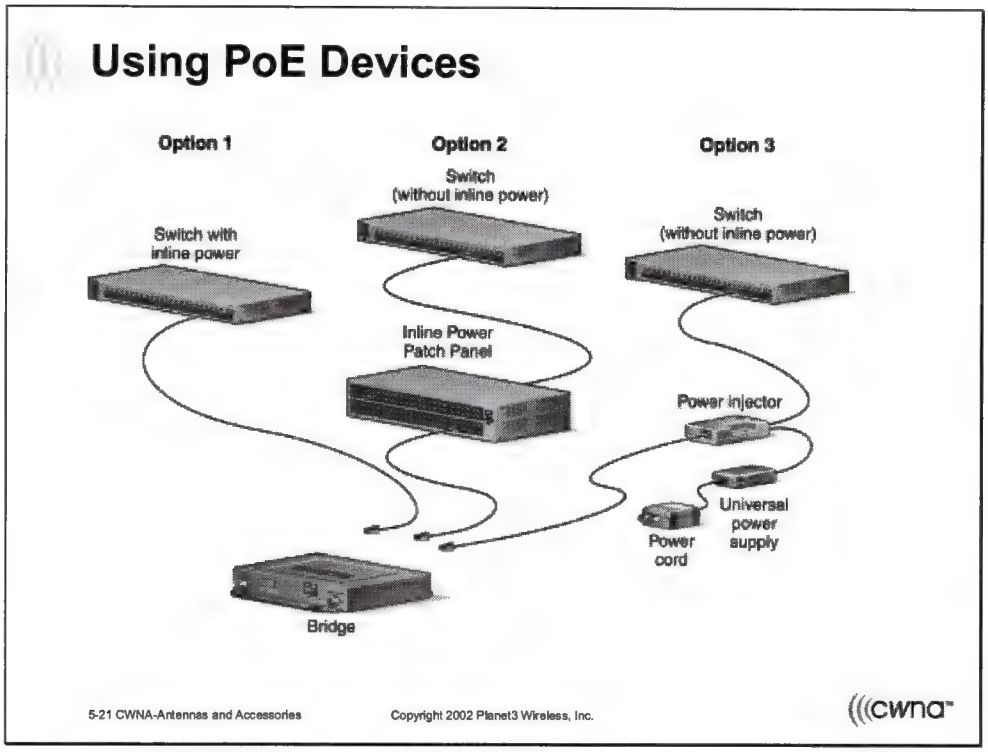


Power over Ethernet (PoE)

Power over Ethernet (PoE) is a method of injecting DC voltage onto the unused pairs in Category 5 (CAT5) cabling to power access points and other network devices in a wireless LAN. In terms of power receptacle installation, PoE reduces the difficulty in getting power to remote locations such as ceilings and rafters. Using PoE, system installers need to run only a single CAT5 Ethernet cable that carries both power and data to each device. PoE allows greater flexibility in the locating of access points and wireless bridges and significantly decreases installation costs of wireless hardware.

PoE devices can come in several forms:

- Single-port DC voltage injectors
- Multi-port DC voltage injectors
- Ethernet switches designed to inject DC voltage onto each port on a given pair of pins



Using PoE (IEEE 802.3af)

Using PoE starts with a power injector that inserts DC voltage onto the CAT5 cable. Installation of the injector usually occurs near the Ethernet switch or hub. Often this location is near a wiring closet due to the availability of AC power receptacles. Access points and other network devices accept the DC power from the CAT5 cable through their RJ45 jack. A device that does this is considered PoE compatible.

PoE requires no configuration. The CAT5 cable is simply plugged into the unit and the unit will function.

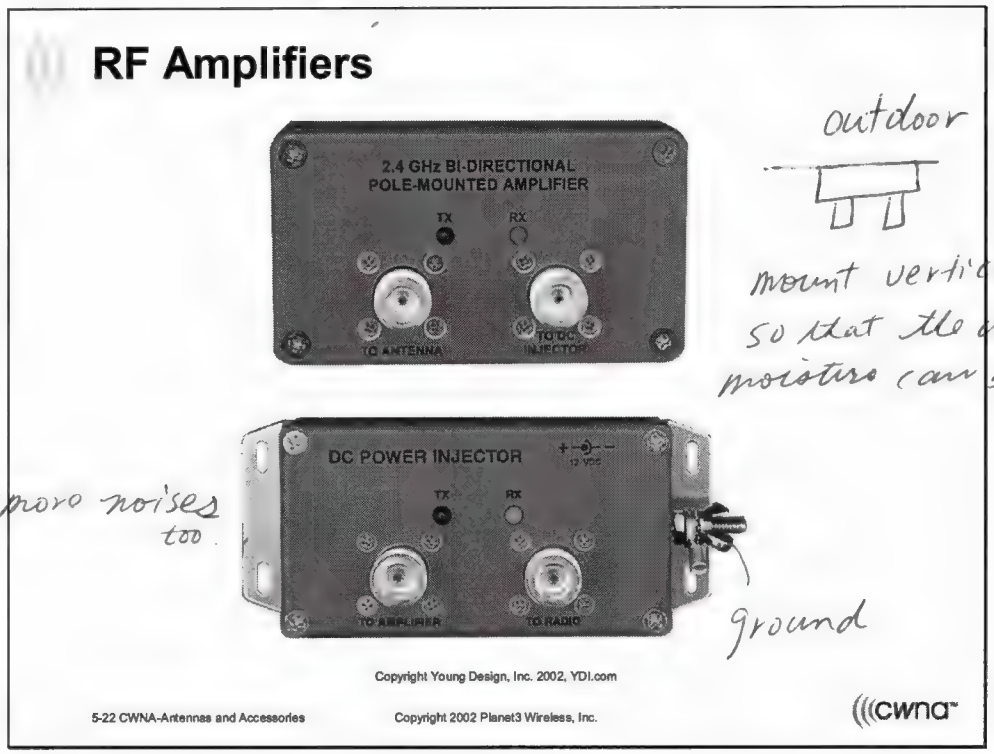
PoE Caveats

PoE is not yet standardized although the IEEE does recommend +48 VDC. Currently the 802.3af Task Force is working to standardize PoE as an official IEEE standard. Currently, different vendors may use different voltages, and there are no standards on which pair of unused pins is to be used in applying the DC voltage. Also, the polarity must be alike before two units will be compatible. When using PoE for the current time, it is recommended to use products from the same manufacturer until a standard is developed and ratified to prevent damaging equipment.

Note Remember that the effective maximum length of a Cat5 cable is 100 meters, thus PoE is not a viable solution for any distance greater than this length.

Copyright © 2003, Planet3 Wireless, Inc.

Wireless LAN Accessories



RF Amplifiers

RF amplifiers are used to increase the signal strength between the transmitter and the antenna along the antenna cable. RF amplifiers precisely amplify (make larger) the RF signal (measured in dBm). Most in-line RF amplifiers are powered using DC voltage along the antenna cable such that the antenna cable is carrying both the high-frequency AC signal and the DC voltage.

Two Types of RF Amplifiers

A *Unidirectional* amplifier offsets the losses created by long antenna cables and connectors by boosting the RF signal before it is propagated from the antenna. Unidirectional amplifiers are losing popularity due to the advantages of Bi-directional amplifiers discussed next.

A *Bi-directional* amplifier aids in boosting the effective sensitivity of the receiver as well as boosting the RF signal to be transmitted. In the case of a 15-mile wireless link, the signal would be very small at the receiving end. With a bi-directional amplifier, the signal is amplified outbound (from transmitter to antenna) and inbound (from antenna to receiver). It is important to place an amplifier close to the antenna so as to offset RF cable loss. Use of linear amplifiers cleanly amplifies the main RF signal while reducing noise and the negative effects of sidebands.

Choosing an RF Amplifier

Amplifiers should be purchased based on how much gain the device will add to the input signal, what frequency range is supported, input and output impedances, and how much input power the unit can take. Manufacturers may provide a calibration report and a certificate for the equipment. The amplifier's accuracy should be verified to ensure that the given amount of gain is actually being produced.

RF amplifiers may be rated for a fixed output power (measured in mW or dBm) or a fixed gain (measure in +dB). RF amplifiers will also have an operational frequency range (measured in MHz or GHz) and should have a flat frequency response across this range. An RF amplifier should be chosen based on the needs of the wireless LAN configuration, and the impedance should match with all other wireless LAN components (usually 50 ohms) in the system.

Copyright © 2003, Planet3 Wireless, Inc.

simpbo.com

RF energies need to get certificate

FCC Certified System Certificate

TCB

GRANT OF EQUIPMENT AUTHORIZATION
Certification
Issued Under the Authority of the
Federal Communications Commission
By:

TCB

Timco Engineering, Inc.
849 NW State Road 45
P.O. Box 370,
Newberry, FL 32669

Date of Grant: 04/12/2002
Application Dated: 04/12/2002

Young Design Inc
8009 Lee Highway
Falls Church, VA 22042
Attention: Michael Young, President

COPY

NOT TRANSFERABLE

EQUIPMENT AUTHORIZATION is hereby issued to the named GRANTEE, and is VALID ONLY for the equipment identified hereon for use under the Commission's Rules and Regulations listed below

FCC IDENTIFIER:
Name of Grantee:

Equipment Class: Part 15 Spread Spectrum Transmitter
Notes: Wireless LAN

Grant Notes	FCC Rule Parts	Frequency Range (MHz)	Output Watts	Frequency Tolerance	Emission Designator
36	15C	5740 - 5811	0.25		

This device must be professionally installed and is authorized for use with 5 antennas, as documented in the filing. The antenna(s) used for this transmitter must be fixed-mounted on outdoor permanent structures with a separation distance of at least 2 meters from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. Users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

36: Certain antennas used with this equipment require a minimum cable length, or have output power limitations as documented in the application.

5-23 CWNA-Antennas and Accessories

Copyright 2002 Planet3 Wireless, Inc.

((cwna

Special Stipulations

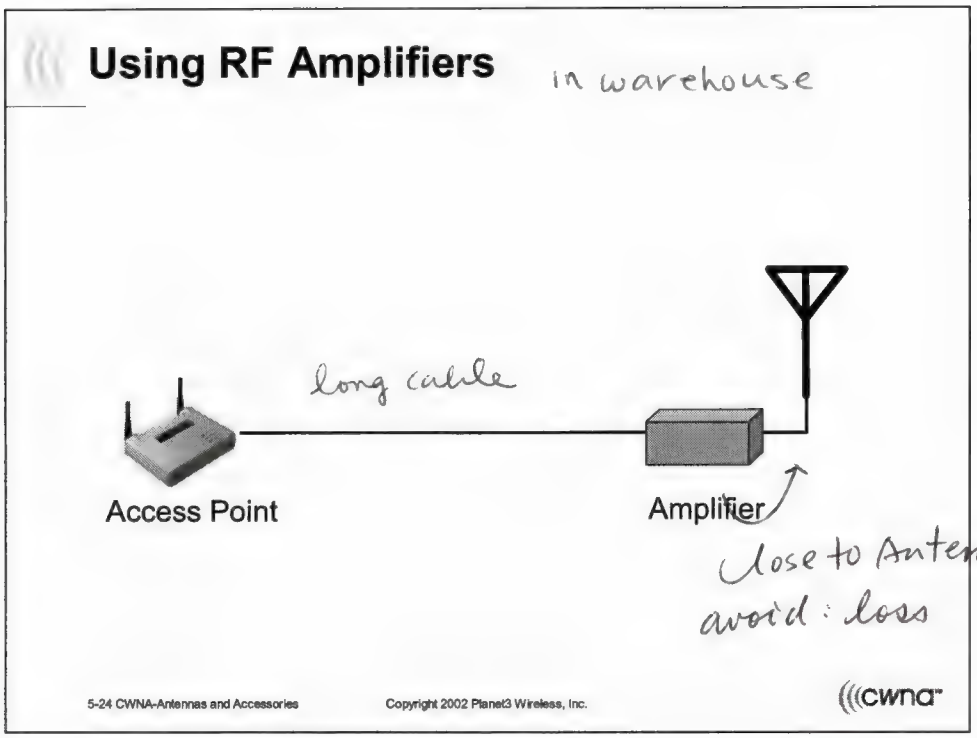
The FCC's CFR 15.204 states that every system must be certified by the FCC for use in the ISM and UNII bands. A "system" is defined as the transmitting device, the cabling, connectors, amplifiers, attenuators, splitters, and the antenna. Manufacturers obtain FCC approval or "certification" of their hardware such that an end-user may purchase any of their radio devices and antennas and use them as a system without contacting the FCC for testing and certification. When additional devices such as amplifiers are added into the circuit, the manufacturer's certification no longer applies and a user must obtain his own certification of his system. This might cost as much as $12,000 per system. An answer to this problem might be to purchase an FCC certified system from a reputable vendor that meets the requirements of the wireless network.

CFR 15.204 does not allow an amplifier to be marketed or sold when not part of a "certified" system. The FCC maintains a database of certified systems and companies holding these certifications. This database can be searched at the following web address: http://gullfoss2.fcc.gov/cgi-bin/ws.exe/prod/oet/forms/reports/Search_Form.hts?form=Generic_Search

This website is meticulously maintained by the FCC, and is always current. Typical updates are a minimum of weekly. The end-user is liable for violations of FCC rules while they use the equipment. FCC violations may result in fines of $27,500 - $1,200,000 per violation. The FCC usually typically allows a violator a brief (e.g. 10 days) time to correct the problem and report to the FCC how the violation was repaired. It is not uncommon for the FCC to audit a Wireless ISP looking for certified system infractions.

Many manufacturers do not produce amplifiers to be used with their systems. For this reason, there are companies that produce amplifiers (but not wireless LAN hardware) that obtain FCC certification of an entire wireless LAN system using their amplifiers and another vendor's wireless LAN hardware together.

Copyright © 2003, Planet3 Wireless, Inc.



Using RF Amplifiers

Setup and Installation

RF amplifiers are placed in series with the main RF signal, which means the signal flows through the amplifier. The devices are typically mounted outdoors with the connectors facing down to keep water out. Drip loops are also used to keep water out of the devices, where a loop in the cable will cause the water to drip downwards. Mounting an RF amplifier can be done outside on the antenna mast or inside on a wall or near the radio. The amplifier should be placed as close to the antenna as possible in order that the amplifier may compensate for cable loss for the return signal.

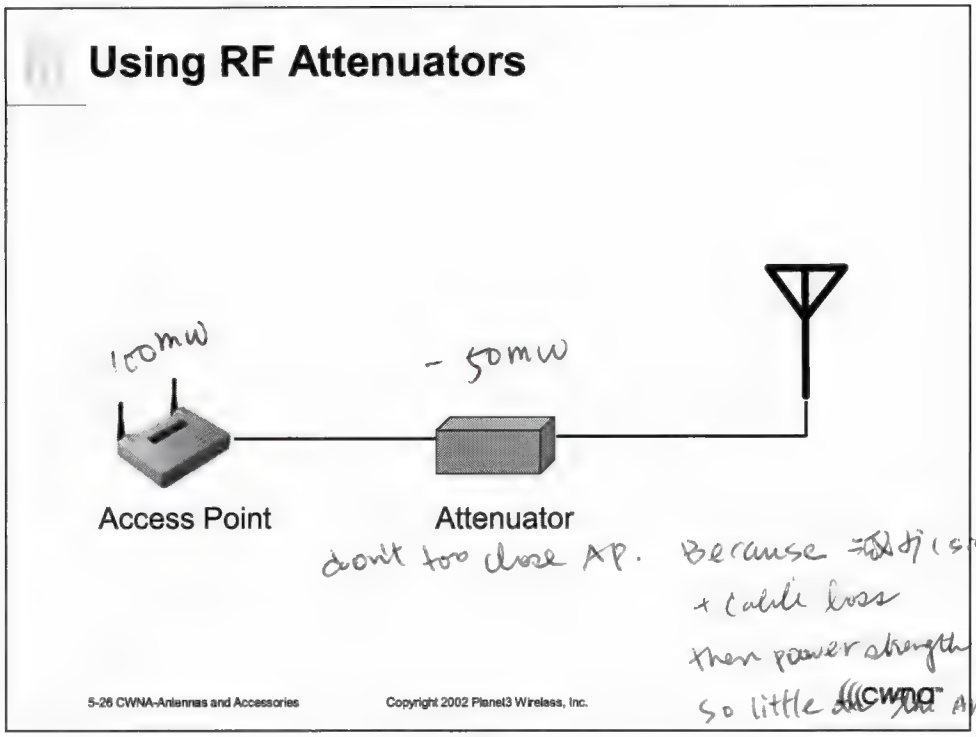
RF Attenuators

An RF attenuator is a device that causes precisely measured loss (in –dB) in an RF signal. While an amplifier will increase the signal, an attenuator will decrease it.

Choosing an RF Attenuator

An attenuator should be purchased based on how much loss the device will introduce into the signal path, how much input power the unit will take, impedance of the attenuator is, and what frequency range is supported. Manufacturers may provide a calibration report and a certificate for the equipment. RF attenuators are rated for a particular input power (mW), impedance (ohms), loss (dB), and frequency range (MHz or GHz) that should be chosen based on the needs of the wireless LAN configuration. The impedances should match with all other wireless LAN components (usually 50 ohms).

Copyright © 2003, Planet3 Wireless, Inc.



Using RF Attenuators

Setup and Installation

Most RF attenuators used with wireless LANs are installed in series with the main signal path. They are typically mounted to a surface with screws through their flange plates if mounting is required at all. Some attenuators simply sit between lengths of cable and are no larger than the cable itself such as the one in the top-left of the photo on the previous page.

Attenuators are not always placed closer to the antenna or the access point. If the attenuator can only take a 50 mW input for example, and the access point was emitting 100 mW of output power, having the attenuator near the access point would be disastrous, possibly causing attenuator failure. In a case like this, placing the attenuator closer to the antenna might mean that the cable loss brings the input power down to acceptable input levels at the attenuator.

Lightning Arrestors

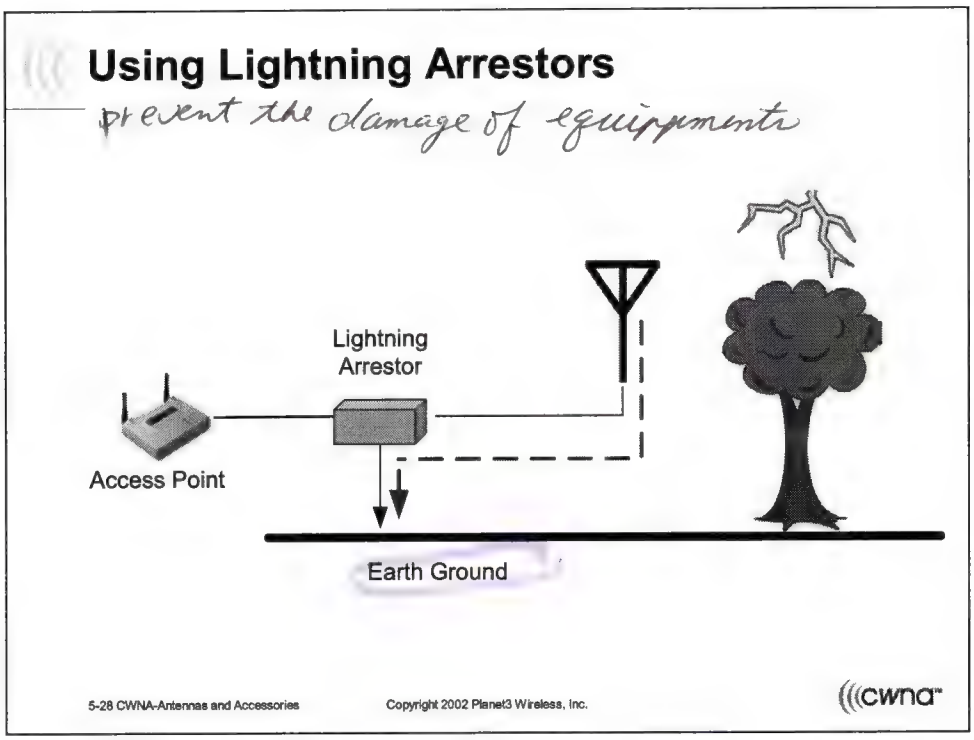
A lightning arrestor is used to shunt (turn aside or move to an alternate course) transient current to Earth ground that is caused by lightning. Transient currents are electrical currents created when lighting strikes a nearby object or area. The primary use of a lightning arrestor is for protecting wireless LAN hardware such as access points, bridges, and workgroup bridges that are attached to a coaxial transmission line.

Lightning arrestors do not support a direct hit from lightning, but can generally shunt surges up to 5000 amperes at up to 50 volts. Most lightning arrestors are capable of shunting more electric current then they will need to handle.

Choosing a Lightning Arrestor

When selecting a lightning arrestor for a wireless network, make sure the unit meets the IEEE standard of <8 uS. Most lightning arrestors conduct at <2 uS, which exceeds the IEEE standard by four times. Look for lightning arrestors that can handle multiple strikes or near strikes, are designed for the correct frequency band, and are the same impedance as the RF system.

Copyright © 2003, Planet3 Wireless, Inc.



Using Lightning Arrestors

The following steps outline how a lightning arrestor works:

1. Lightning strikes a nearby object
2. Transient currents are induced onto the main RF signal line via the coaxial cable or the antenna.
3. The lightning arrestor senses these currents and immediately ionizes the gasses held internally, causing a short (a path of almost no resistance) directly to Earth ground.

Ground Antenna outdoor

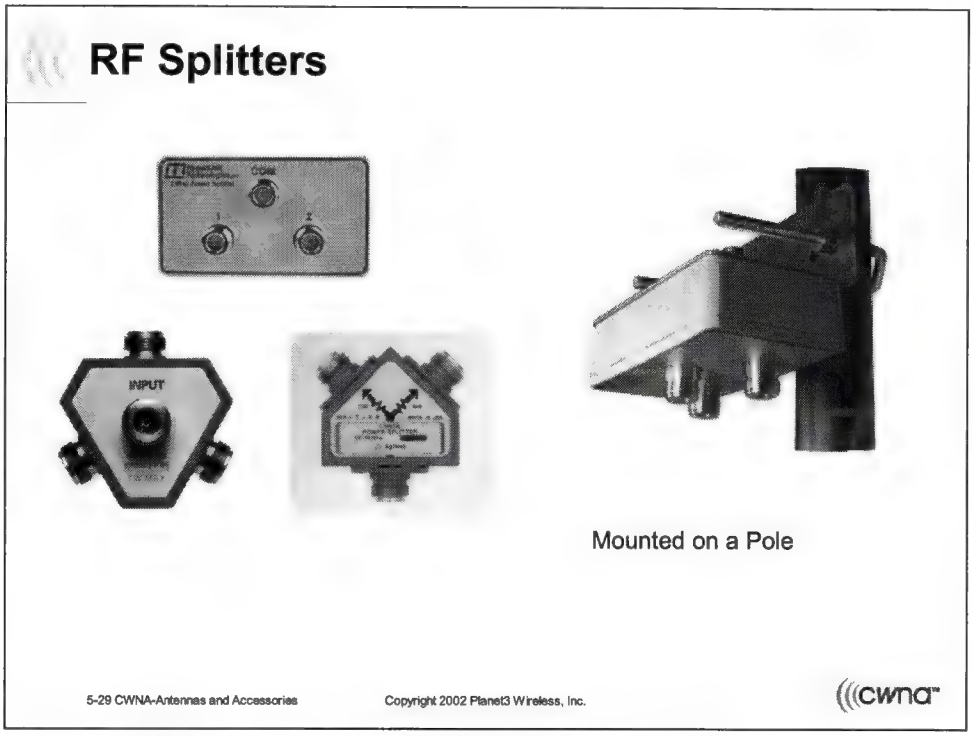
Note It is important to attach lightning arrestors to good Earth ground to ensure proper function. A good Earth ground is considered to be 5 ohms or less.

Setup and Installation

Lightning arrestors are installed in series with the main RF signal. The grounding connection should be attached to the best possible Earth ground.

Lightning arrestors are usually designed so that when they fail, they block the signal to the antenna. Some may have a replaceable gas discharge tube while others require that the entire arrestor be replaced. In some cases, they are designed to handle multiple strikes without failure. Additionally, some are designed for no maintenance at all, even after a strike. One can normally see if a unit is bad because the unit is charred. A lightning arrestor may fail open or shorted.

Copyright © 2003, Planet3 Wireless, Inc.



RF Splitters

An RF splitter is a device that has a single input connector and multiple output connectors. An RF splitter is used for the purpose of splitting a single RF signal into multiple independent RF signals. Splitters are not powered devices. The types of connectors on an RF splitter are generally an N-type or SMA. Specific uses of splitters include bi-directional coverage along a river or road at long distances using directional antennas.

A splitter can split a signal 2 ways, 3 ways, 4 ways, or however many ways the hardware allows. For example, if a splitter is splitting 4 ways, the power from the input is divided 4 ways resulting in each of the outputs getting ¼ of the power. Using splitters is generally not recommended due to this particular issue. In this scenario, each split actually does not get the full ¼ of the output. Due to insertion loss, the input power is automatically reduced by a given amount before the power is split 4 ways. This might, for example, actually equate to each of the 4 outputs having 1/5 of the input power instead of ¼ of the input power. In a typical 2-way splitter, one might expect to lose up to 4 dB between the input and either output connector.

Choosing an RF Splitter

Good quality RF splitters will have high isolation impedance between ports and low insertion loss (measured in dB). Splitters are rated for power input maximums. Exceeding the maximum power input will cause damage to the unit.

All unused ports should be properly terminated. Good quality terminations are important in avoiding reflected power.

Copyright © 2003, Planet3 Wireless, Inc.

RF splitters are specified for use at given frequency ranges. The frequency range should be within the same frequency range as the wireless LAN being used. A splitter that is rated up to 2.0 GHz would not function in a wireless LAN that was working in the 2.4-2.5 GHz range. In this case, the signal might not go through at all.

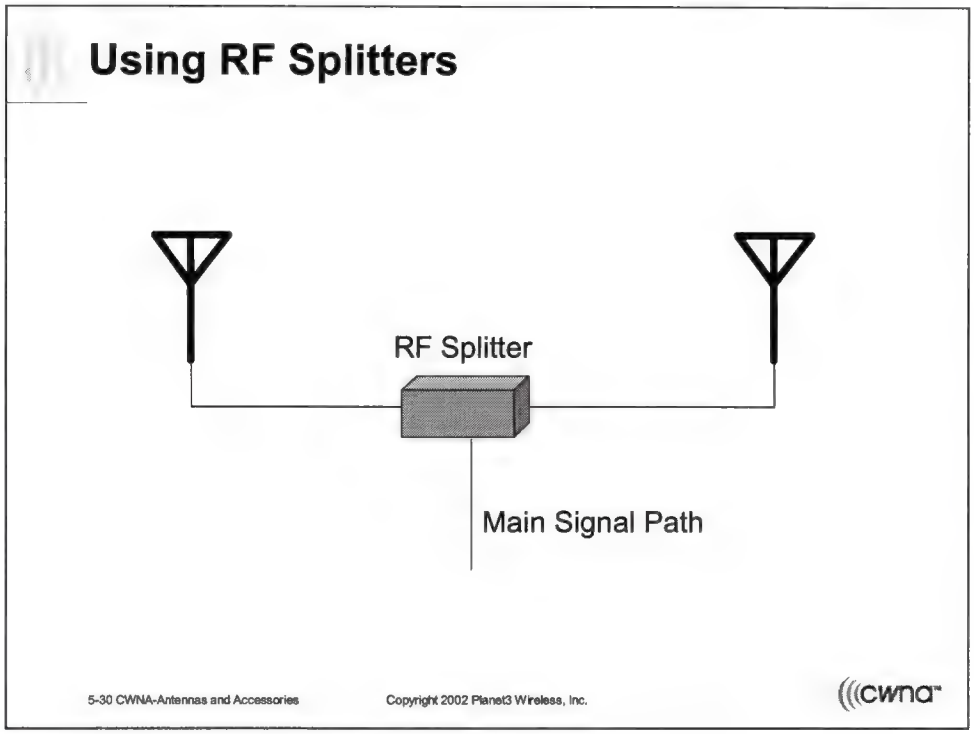
When selecting an RF splitter, the impedances should match with all other wireless LAN components in the configuration (generally 50 ohms) otherwise reflected power will result.

Calibration reports are important to receive when purchasing an RF splitter. This calibration report will show the insertion loss, as well as how flat the frequency response is. Splitters should be purchased with the right type of connectors such as n-type or SMA. Not doing so will require additional connectors that will result in additional signal loss and variable frequency response characteristics.

To use a splitter used as a combiner is not recommended for wireless LANs for the reason that the signal being received by the antenna will be competing directly against signals being put into the second output connector by another access point. Even if the two access points use channels 1 and 11, the sidebands of each channel will still be high enough at the opposing channel's frequency range to interfere with received signals from remote nodes.

In order to use a splitter, the entire system must be FCC certified using the splitter as part of the system. Use of splitters is NOT recommended when it can be avoided.

Copyright © 2003, Planet3 Wireless, Inc.



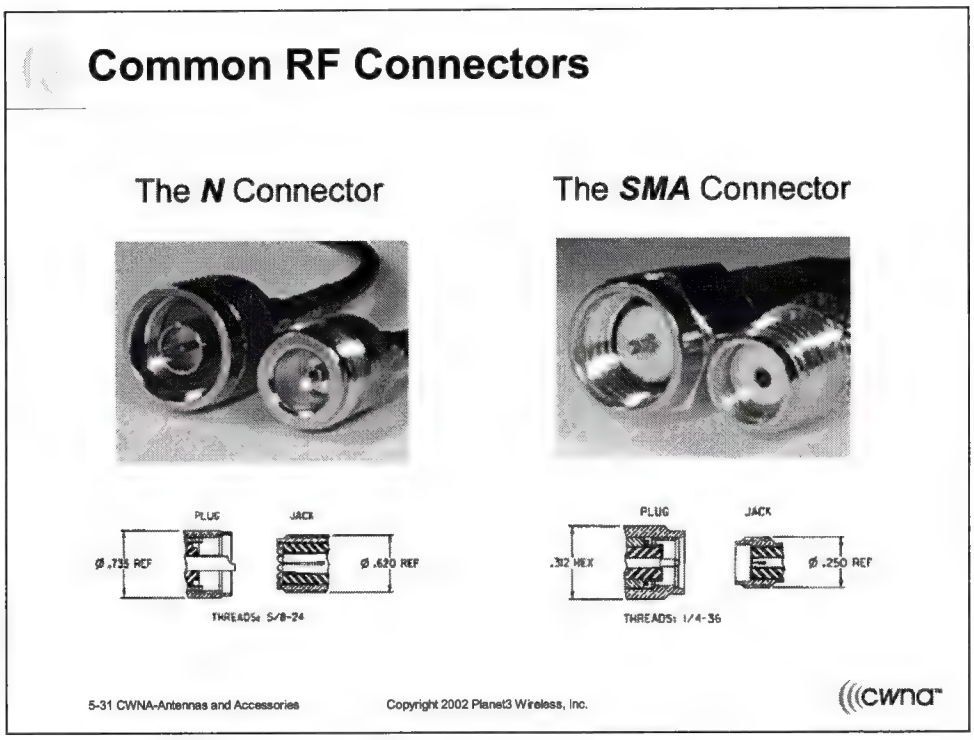
Using RF Splitters

An RF splitter splitting the main signal into 2 separate signal paths is illustrated above. The two resultant signals then feed into antennas for transmission.

Setup and Installation

When installing an RF splitter, the input connector should always face the source of the RF signal. The output connectors are connected facing the destination of the RF signal (a receiver or antenna).

Copyright © 2003, Planet3 Wireless, Inc.



RF Connectors

RF connectors are specific types of connection devices used to connect cables to devices or devices to other devices. Traditionally, N-type and SMA-type connectors (or derivatives) have been used with wireless LANs.

FCC Guidelines

In 1994 the FCC and DOC (now "Industry Canada") ruled that connectors for use with wireless LAN devices should be proprietary between manufacturers. For this reason, there are many variations on each connector type such as:

- N-type
- Reverse polarity N-type
- Reverse threaded N-type

This rule was created because the FCC wanted to assure all RF systems are certified. This ruling reduces accidental violations of FCC maximum power output and power density rules. Manufacturers submit their systems to the FCC for certification so that any of their radio devices (access points, bridges, etc.) will be certified with any of their antennas. This allows consumers to easily stay in compliance with FCC rules.

Choosing an RF Connector

When selecting an RF connector, the impedances should match with all other wireless LAN components in the configuration (generally 50ohms) otherwise reflected power can result.

A connector's insertion loss must also be taken into consideration. A connector added to the signal path can yield as much as ½ dB loss.

Connectors have frequency limit specifications. Purchase only those connectors that are capable of handling frequencies at which the wireless network is operating.

Note Purchase high-quality RF Connectors from a reputable company. Connectors are not usually calibrated, and cheap RF Connectors can impact loss and can even affect frequency response.

Setup and Installation

If RF connectors are installed outdoors, use commercial grade electrical tape or sealant to avoid water leakage into the connector (or cable) that would ruin the connection. Prior to sealing, the configuration should be thoroughly tested, including the following:

- Verifying the signal levels are correct
- Verifying that data can be transmitted

Note Installation of outdoor connectors and cabling should be done in dry weather when the connections can be sealed without accidentally sealing in water.

Copyright © 2003, Planet3 Wireless, Inc.

LMR Coaxial Cable Attenuation Ratings

Nominal Attenuation In dB/100 Feet At (MHz)

LMR CABLE	30	50	150	220	450	900	1500	1800	2000	2500
100A	3.9	5.1	8.9	10.9	15.8	22.8	30.1	33.2	35.2	39.8
195	2.0	2.6	4.4	5.4	7.8	11.1	14.5	16.0	16.9	19.0
200	1.8	2.3	4.0	4.8	7.0	9.9	12.9	14.2	15.0	16.9
240	1.3	1.7	3.0	3.7	5.3	7.6	9.9	10.9	11.5	12.9
300	1.1	1.4	2.4	2.9	4.2	6.1	7.9	8.7	9.2	10.4
400	0.7	0.9	1.5	1.9	2.7	3.9	5.1	5.7	6.0	6.8
400UF	0.8	1.1	1.7	2.2	3.1	4.5	5.9	6.6	6.9	7.8
500	0.54	.70	1.2	1.5	2.2	3.1	4.1	4.6	4.8	5.5
600	0.42	.55	1.0	1.2	1.7	2.5	3.3	3.7	3.9	4.4
600UF	0.48	.63	1.15	1.4	2.0	2.9	3.8	4.3	4.5	5.1
900	0.29	0.37	0.66	0.80	1.17	1.70	2.24	2.48	2.63	2.98
1200	0.21	0.27	0.48	0.59	0.89	1.3	1.7	1.9	2.0	2.3
1700	0.15	0.19	0.35	0.43	0.63	0.94	1.3	1.4	1.5	1.7

5-32 CWNA-Antennas and Accessories Copyright 2002 Planet3 Wireless, Inc. cwna

Large diameters

500 feet 1700 LMR → 60 dollars

RF Cables

The most commonly used RF cables in wireless LANs are low-loss high-frequency rated cables such as LMR. There are other types of cables available, but LMR cables are recommended for their performance.

The attenuation ratings in the above table serve as a reference guide when computing the loss of signal introduced for specific lengths of cable at particular frequencies.

Choosing RF Cables

When selecting an RF cable, the impedance should match with all other wireless LAN components in the configuration (generally 50 ohms) otherwise reflected power can result.

Cables always introduce loss to the wireless LAN RF signal, so the lengths of the cable should be kept as short as possible. As more cable is added to the wireless LAN, more signal loss is introduced.

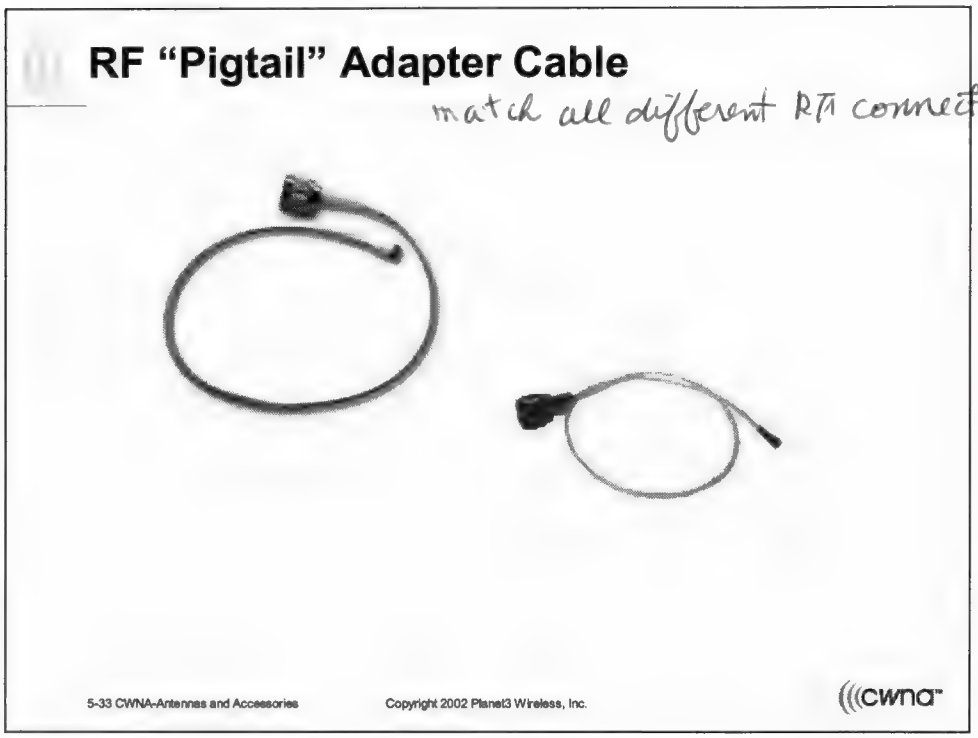
Purchase pre-cut lengths of cable with pre-installed connectors when possible. Trying to put RF connectors on RF cables without the proper equipment and then testing it without the proper testing equipment to make sure return loss (VSWR) will not occur is not recommended except for professional cable manufacturers. Manufacturers' equipment is reliable and manufacturers are better equipped to perform this task. If the correct length of cable cannot be obtained, use connectors to make the cable the necessary length by combining multiple cables. Most manufacturers will sell connectors and cables with the antenna equipment.

Usually, the accessories will come at a premium price but the purchase will save time and money compared to what it would take to make cables and troubleshoot problems associated with improper cable manufacturing.

Look for the lowest loss cable available within the budget constraints (the lower the loss, the more expensive the cable). Cables are typically rated for loss in dB/foot.

Keep in mind that the FCC certifies entire systems that include the type and lengths of RF cable. For this reason, it is highly recommended preconfigured cable lengths from the manufacturer of the wireless LAN hardware used should be purchased to ensure that the customer and end-user would be in compliance with FCC regulations.

Copyright © 2003, Planet3 Wireless, Inc.

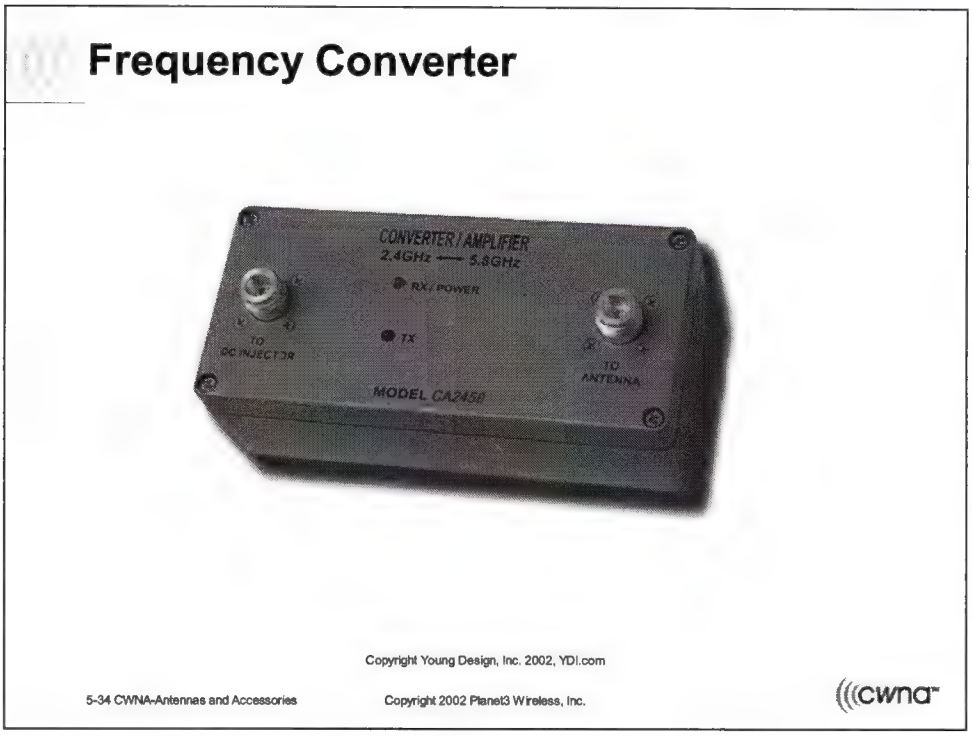


RF "Pigtail" Adapter Cable

In most cases, pigtails are used to adapt proprietary connectors to industry standard connectors like N-type and SMA connectors. On one end of the cable is the proprietary connection and on the other is the standard connection. There are occasions where adapting an industry standard to a different type of industry standard connector will be necessary, but the FCC has special rules regarding use of industry standard connectors in a wireless LAN.

Note Pigtails are sometimes used to circumvent the 1994 DOC/FCC ruling on proprietary connectors for manufacturers. This is both illegal and not recommended.

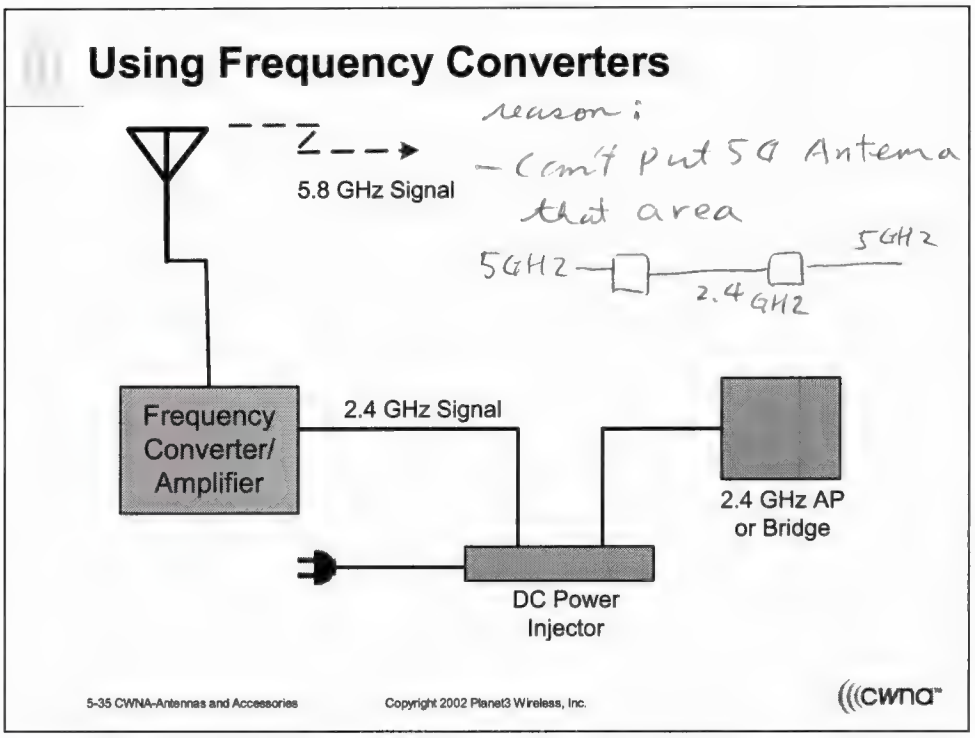
Copyright © 2003, Planet3 Wireless, Inc.



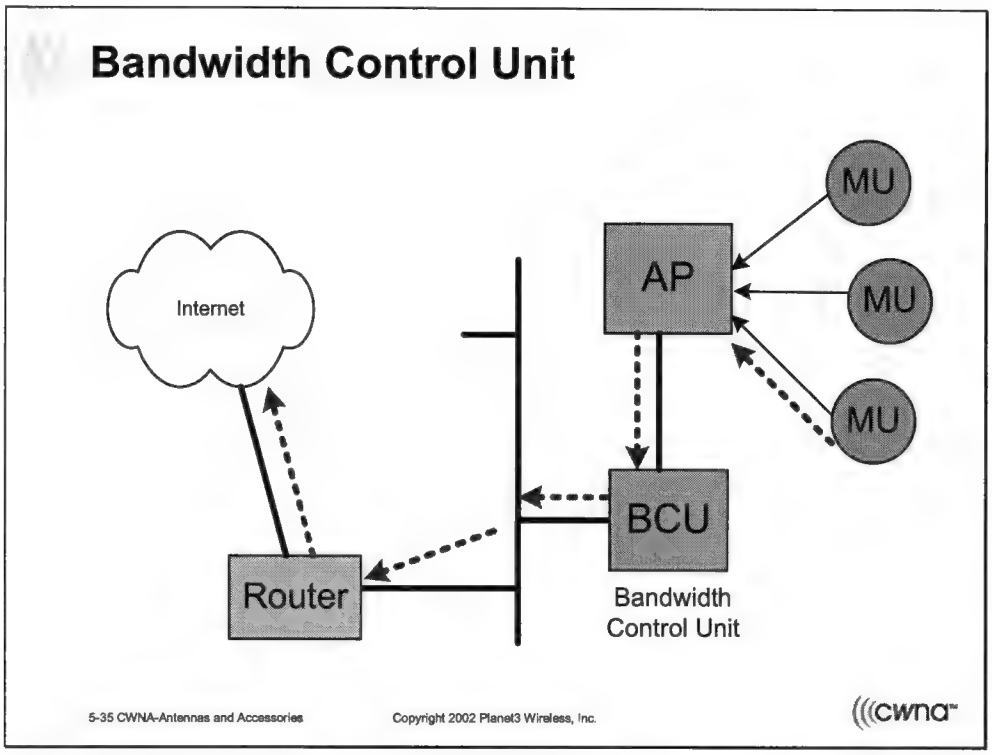
Frequency Converter

Frequency converters are used for converting one frequency range to another for the purpose of decongesting a frequency band. Suppose many companies that were located in the same multi-tenant office building had wireless LANs (which is common). Each of these companies wants building-to-building wireless connectivity with a building next door because each of these companies have an office in the adjacent building. It is easy to see that only 3 companies will be able to use wireless LAN building-to-building bridging due to a limited number of non-overlapping channels. In this case, a frequency converter may be deployed that will use existing 2.4 GHz wireless equipment, but will convert the frequencies to a less congested band (such as the 5.8 GHz upper UNII band) for this wireless bridge segment.

Copyright © 2003, Planet3 Wireless, Inc.



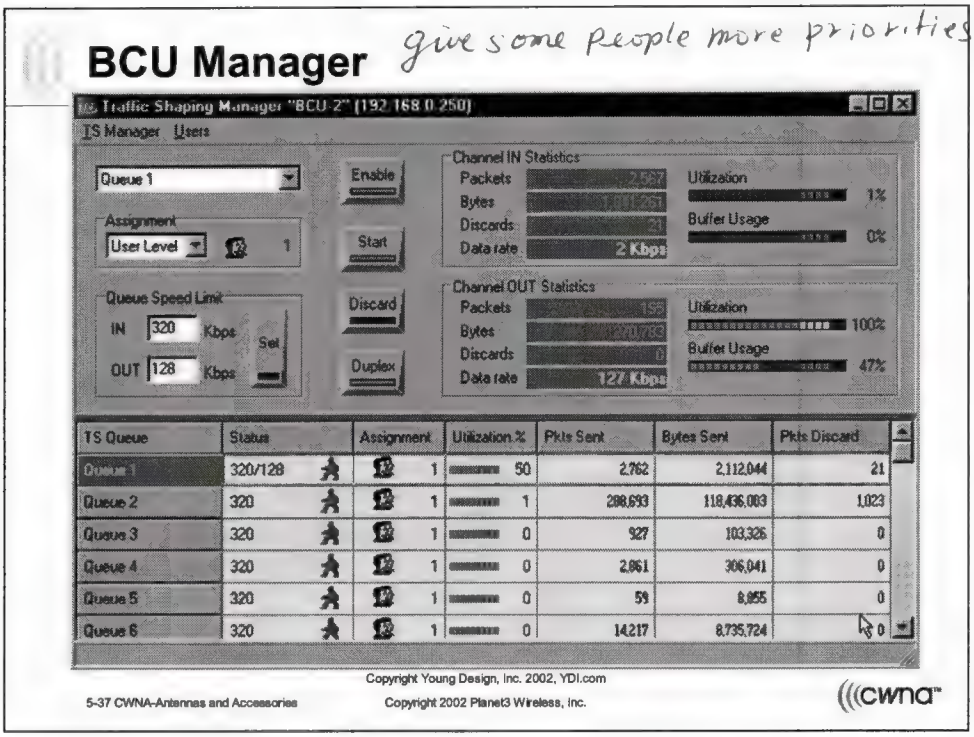
Proper antennas and cables must be used when using a frequency converter due to both antennas and cables having limited frequency response, but it can be a very economical solution in a congested area. The alternative would be to replace all wireless LAN hardware with new 5 GHz hardware.



Bandwidth Control Units

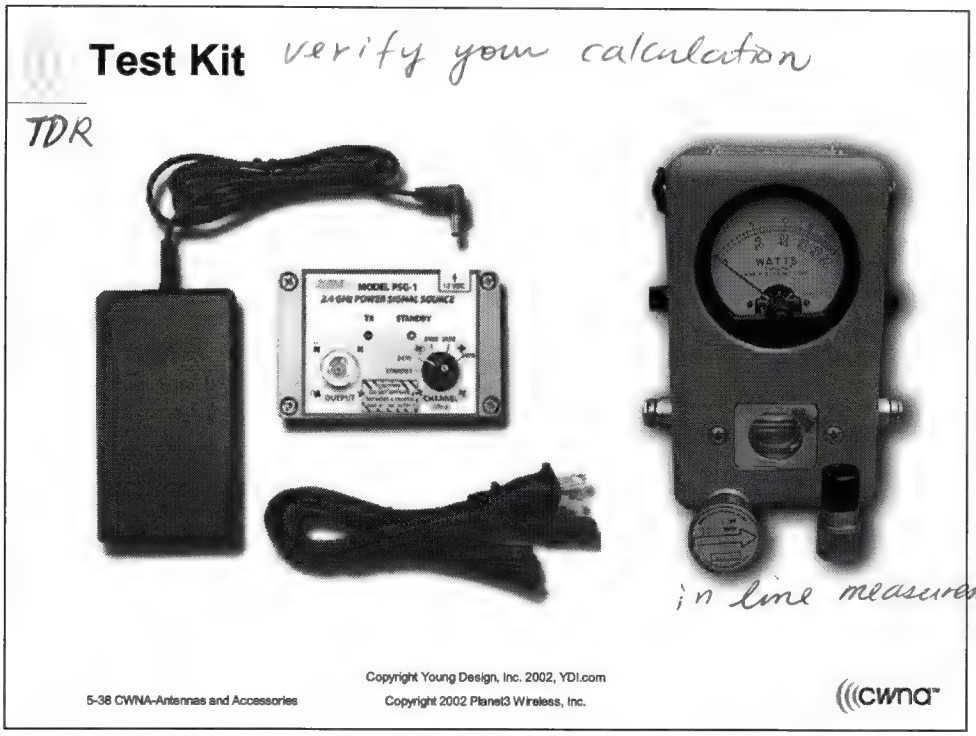
Wireless LANs are a shared medium with very low throughput in comparison with today's wired LAN technologies. For this reason, bandwidth on wireless LANs must be conserved and protected - especially in outdoor environments such as would be found with wireless Internet service providers (WISPs). Bandwidth should be controlled in such a manner that each user has a reliable and consistent connectivity experience and gets what they are paying for. With indoor wireless LAN installations, it is not as common to use a Bandwidth Control Unit (BCU) because many users are expecting to have the same experience as they had on the wired LAN. This simply isn't feasible considering the extreme bandwidth differences. However, administrators strive to give indoor LAN users as much bandwidth as possible by not overloading access points.

Copyright © 2003, Planet3 Wireless, Inc.



Bandwidth Control Units

BCUs typically work by filtering on MAC addresses in order to drop each user into a pre-assigned queue. Each queue has particular properties such as upstream and downstream bandwidth. Multiple users might be put into the same queue. This allows for precise bandwidth control and accounting per user.



Test Kits

There are many types of test kits on the market. One of the most valuable types of test kits in the wireless LAN industry is one used for testing cables and connectors. The kit might consist of an RF signal generator and a through-line power meter. The signal generator can be hooked directly to the power meter to get a baseline measurement. When putting cables and connectors between the signal generator and the power meter, it can be determined if they meet the manufacturer's specifications and if they are intermittent. The connectors on cables can become worn and loose making a bad or intermittently bad connection. They can also take on water, which would be highly detrimental to their RF characteristics. It is important to test cables and connectors before deployment and periodically as possible thereafter.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

6 Wireless LAN Organizations and Standards

Objectives

Upon completion of this chapter you will be able to:

- Define what regulations the FCC creates
- Explain what the ISM and UNII bands are and how they are used
- Define the different 802.11 standards and drafts as set forth by the IEEE
- Describe the competing technologies for wireless LANs

6-2 CWNA-Wireless LAN Organizations and Standards

Copyright 2002 Planet3 Wireless, Inc.

Chapter Content

Because wireless transmissions are governed by law, wireless LAN administrators need to know what these rules and regulations are in order to make sure their wireless configurations are within the parameters of the law. Failure to do so can result in fines or operational shutdown.

Wireless technologies are being implemented at a rapid pace, creating the need for new technologies and features within existing technologies. The forthcoming standards and changes being made in the wireless LAN industry will directly impact the administrators that need to implement and maintain these new technologies.

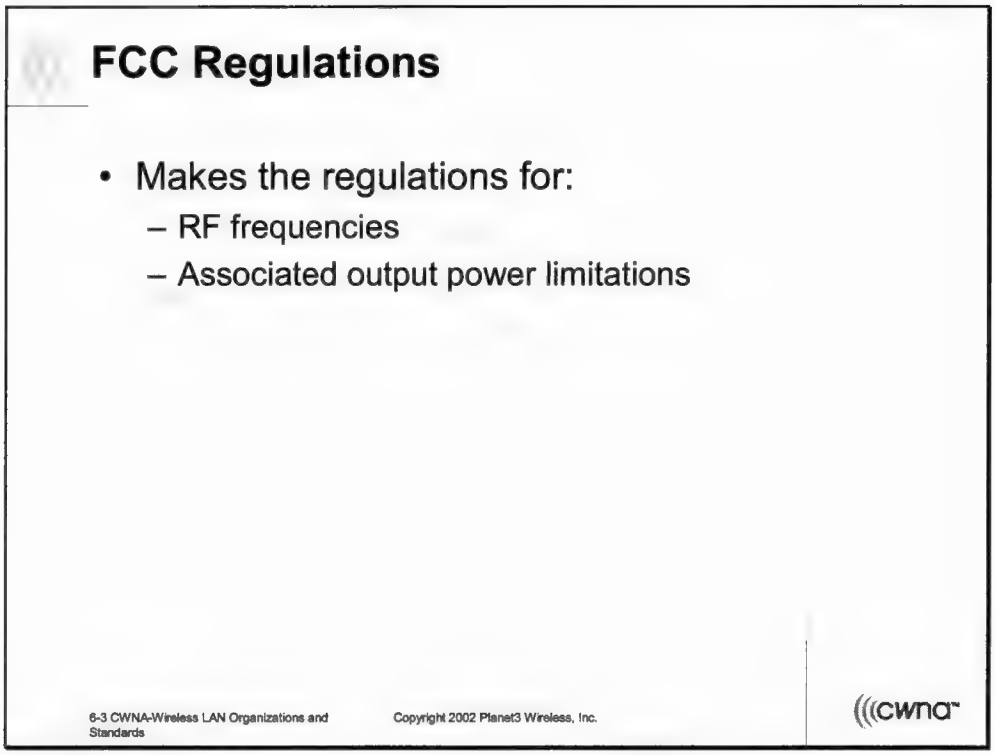
This chapter explains the regulations that govern wireless LAN usage, and how the laws impact the standards being created for the wireless industry. The transmission bands that are available for use are discussed along with which bands each of the standards and drafts use. The chapter ends with a look at the emerging and competing wireless technologies that are becoming available and the role they will play.

The chapter outline follows:

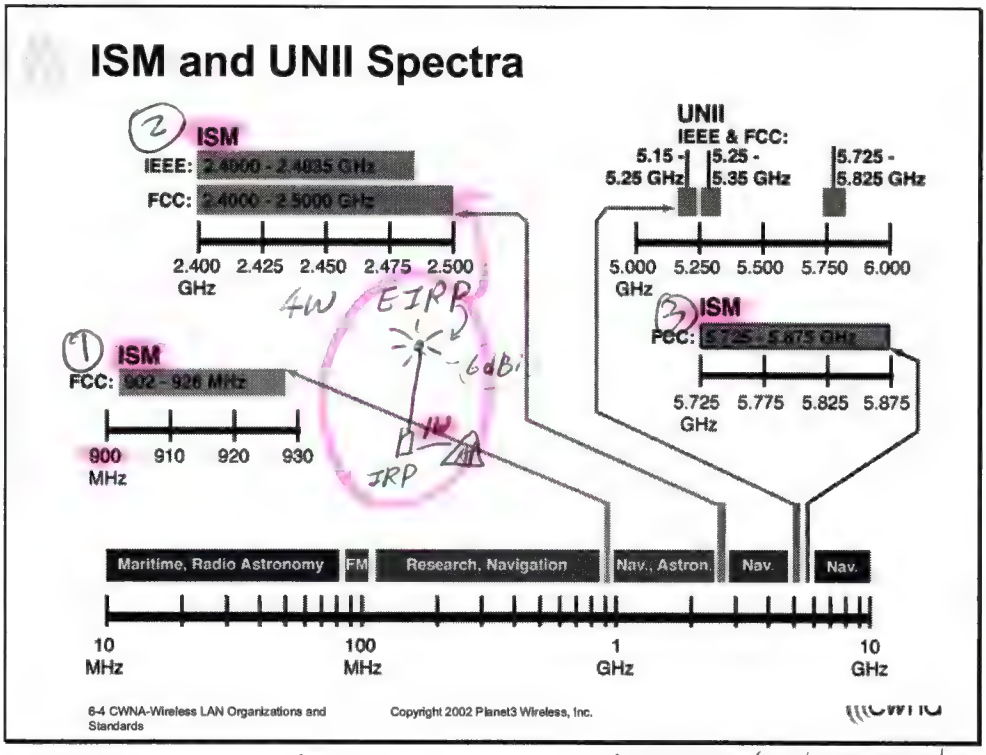
- FCC Regulations
- ISM And UNII Bands And Their Uses
- 802.11 Standards And Drafts
- Competing Wireless Technologies

Copyright © 2003, Planet3 Wireless, Inc.

Federal Communications Commission



The Federal Communications Commission (FCC) made the commercial development of radio-based LAN components possible by authorizing the public use of various transmission bands. In doing so the FCC set regulations that manufacturers had to follow so as to not to interfere with other types of radio equipment, such as cellular phones. The FCC places limitations on the RF frequencies that can be utilized for radio transmission, as well as limitations on the output power used to transmit on those frequencies.



ISM and UNII Bands

The FCC authorized the Industrial, Scientific, and Medical (ISM) radio frequency bands for wireless LAN use. The Unlicensed National Information Infrastructure (UNII) bands are a segment of RF frequencies allocated by the FCC for unlicensed data communications.

These bands are license free, which makes them attractive to manufacturers of wireless LAN hardware. License-free bands do not require the user to register or pay for using the RF frequencies in order to operate equipment that uses the frequencies. The disadvantage of license free bands is that one organization's wireless LAN can interfere with another organizations' wireless LAN. As a network administrator, one has no legal recourse against the interfering organization.

ISM Bands

There are three ISM bands consisting of the 900 MHz band, the 2.4 GHz band, and the 5.8 GHz band. 900 MHz systems are seldom used today due to expense and lack of speed and features. 2.4 GHz systems are widely used, and the 5.8 GHz ISM band is not used for wireless LANs. The 5.8 GHz band overlaps the upper UNII band that is used for 802.11a wireless LANs.

The ISM band at 900MHz is where most wireless LAN equipment started out. This equipment did not have much throughput due to the limited frequency range. The 900 MHz ISM frequencies for wireless LANs reside in the bands between 902MHz and 928 MHz, just above cellular phone frequencies. DSSS and FHSS

Copyright © 2003, Planet3 Wireless, Inc.

equipment is manufactured to work in the 2.4GHz ISM band. Most 900 MHz wireless LAN gear has been replaced by the more modern 2.4 GHz systems.

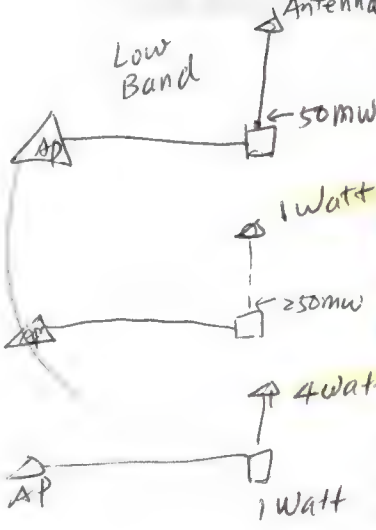
The 2.4GHz ISM band, when configured in a point-to-multipoint scenario, is limited to 1 Watt at the intention radiator, which is the output of the transmitter as measured at the input of the antenna, and 4 Watts EIRP. With a 1 Watt limit at the intentional radiator, a 6 dBi antenna can be used to reach the limit of 4 Watts EIRP.

The FCC states that the 2.4 GHz ISM band spans 2.4 GHz – 2.5 GHz. The IEEE standards allow for use of 2.4 GHz – 2.4835 GHz because the FCC has specified power output only up to 2.4835 GHz.

The 5 GHz ISM band, as defined by the FCC, spans 5.725 GHz – 5.875 GHz. While the FCC allows spread spectrum systems in this band, there are no currently defined standards using these frequencies. The FCC only defines power output from 5.725 GHz to 5.850 GHz, effectively limiting the usable band. This band overlaps with the upper UNII band as defined below. There are standards using the upper UNII band for wireless LANs.

An important change was made by the FCC on May 16, 2002 that opens the 915 MHz, 2.4 GHz and 5.7 GHz ISM bands to new unlicensed spread spectrum devices other than FHSS and DSSS devices. These changes will allow for new digitally modulated systems to operate in these ranges, providing data rates that are much higher than currently available. These modulation systems could turn out to be something similar to the OFDM that is used in 802.11a and 802.11g compliant systems (802.11g is directly affected by this ruling) to reach data rates of up to 54 Mbps. While the appearance of new devices that take advantage of this change has yet to occur, it is expected that WISPs (Wireless ISPs) will be among the first to develop and implement solutions using the newly relaxed rules. These products must comply with an FCC mandated maximum peak output power limit of 100 mW.

UNII Bands



There are 3 UNII bands used by wireless LANs as specified by the FCC in 47 CFR 15.407:

- Lower Band (UNII-1) – 50 mW @ the Intentional Radiator, (5.15 – 5.25 GHz), used indoors only (fixed antennas only), 200 mW EIRP (PtMP)
- Middle Band (UNII-2) – 250 mW @ Intentional Radiator, (5.25 – 5.35 GHz), used both indoors and outdoors, 1 Watt EIRP (PtMP)
- Upper Band (UNII-3) – 1 Watt @ Intentional Radiator, (5.725 - 5.825 GHz), used outdoors only, 4 Watts EIRP (PtMP)

Each UNII band is 100MHz wide, and equipment being made for use in these bands uses OFDM technology, typically complying with the IEEE 802.11a standard. These power levels are for point-to-multipoint systems.

Copyright © 2003, Planet3 Wireless, Inc.

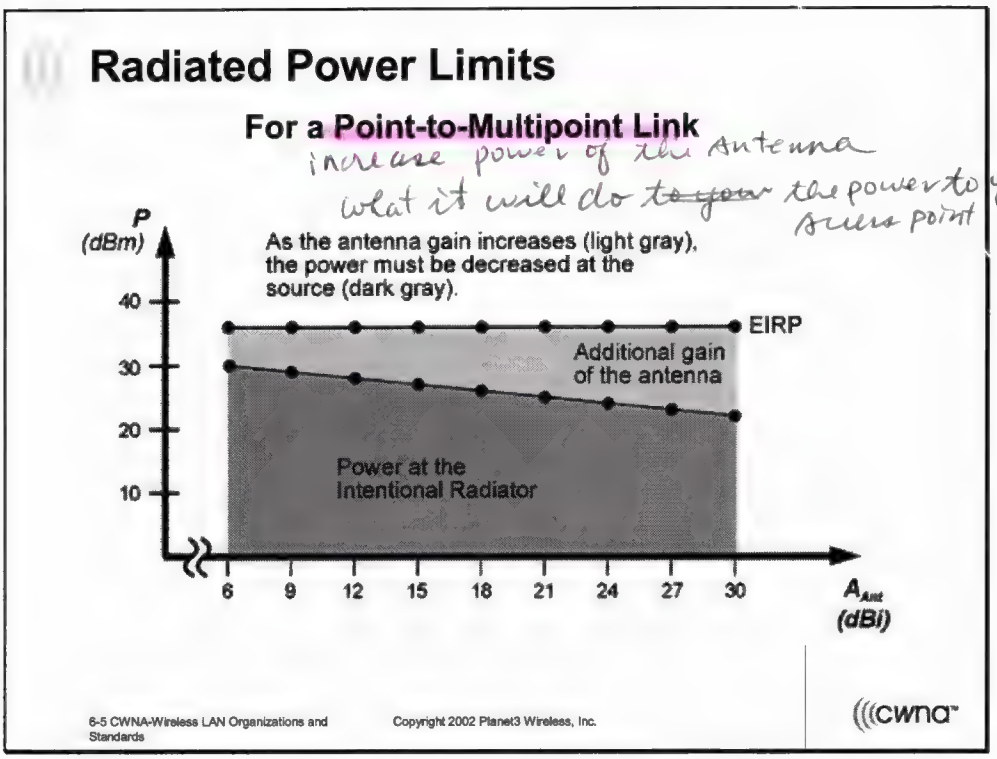
The 802.11a standard specifies use of 20 MHz wide channels with 5 MHz of separation between channels. This standard allows for 4 non-overlapping co-located systems within each UNII band. This is a vast improvement over DSSS systems in the 2.4 GHz ISM band in which there are only 3 non-overlapping channels, each of which is 22 MHz wide. This difference allows greater throughput in the UNII bands, more co-located systems, and less likelihood of interference since UNII band use (traffic) is minor in comparison to the extreme popularity of the 2.4 GHz ISM band.

802.11a

802.11b

Copyright © 2003, Planet3 Wireless, Inc.

thick Access point
(dumb)



FCC Point-to-Multipoint Rules for the 2.4 GHz ISM band

This diagram illustrates how EIRP must always stay the same in a point-to-multipoint system. If the gain on the antenna is increased, the power must be decreased to maintain the FCC requirement of less than 4 Watts EIRP.

There are two rules by which one must abide in order to remain within the laws governing point-to-multipoint wireless systems. The FCC regulation for a point-to-multipoint link allows only 30 dBm (1 Watt) at the intentional radiator and 36 dBm (4 Watts) EIRP. Neither of these rules can be violated.

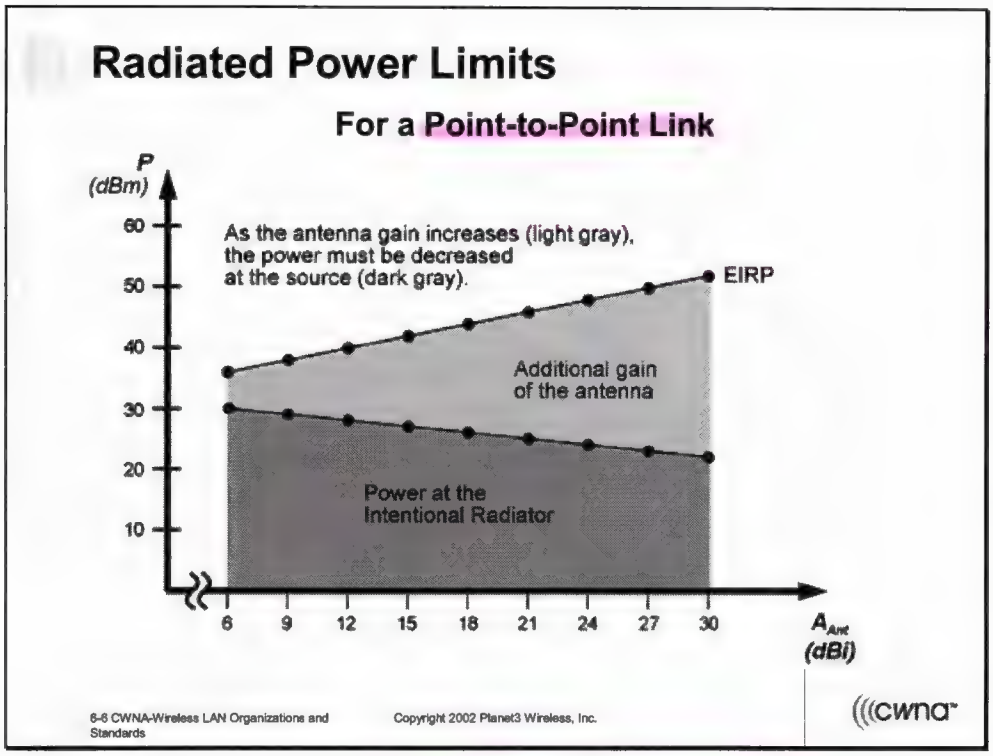
For example, if a 10 dBi antenna were being used, the transmitter would be limited to 26 dBm (10 +26 = 36 dBm). For a 14 dBi panel antenna, the regulation would allow a 22 dBm transmitter. Power is measured at the antenna's input connector, so any cable loss between the transmitter and the antenna must be subtracted. Refer to the following table:

1 : 1
3dBm = 3dBi
= 1 : 1

Power at Antenna (dBm)	Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
27	9	36	4
24	12	36	4
21	15	36	4
18	18	36	4
15	21	36	4
12	24	36	4

-3dBm +3dBi
decrease increase

36 dBm = 10+10+10+3+3 dBm
10 → 10 mW
10 → 1000 mW
10 → 1000 mW
3 → 2000 mW



FCC Fixed Point-to-Point Rules for the 2.4GHz ISM band

FCC regulations (Part 15.247) state that at maximum output power for the intentional radiator (+30 dBm), for every +3 dBi of gain over the initial +6dBi of gain of the antenna system, the power must be reduced at the intentional radiator by -1 dB, thus forming a non-linear relationship between the intentional radiator and the antenna system. Power is measured at the antenna connector, so any cable loss between the amplifier and the antenna must be subtracted.

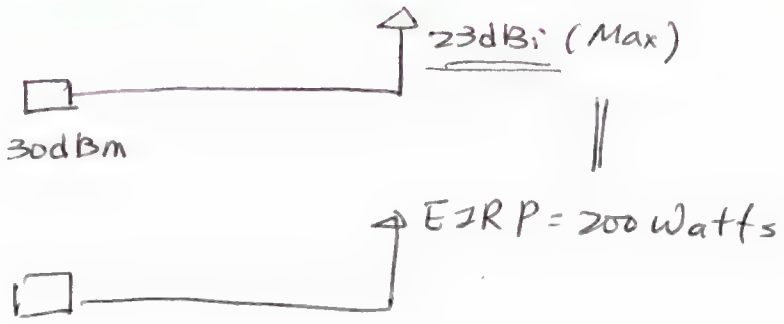
For a point-to-point wireless link, the configuration typically has a directional antenna at each end of the connection. Point-to-multi-point is a 1:1 ratio; whereas for point-to-point there is a 3:1 ratio in that a 3 dBi of antenna gain must be followed by a -1 dB reduction in output power. Refer to the following table:

Power at Antenna (dBm)	Max Antenna Gain (dBi)	EIRP (dBm)	EIRP (watts)
30	6	36	4
29	9	38	6.3
28	12	40	10
27	15	42	16
26	18	44	25
25	21	46	39.8
24	24	48	63
23	27	50	100
22	30	52	158

Copyright © 2003, Planet3 Wireless, Inc.

FCC Fixed Point-to-Point Rules for the upper 5 GHz UNII band

Fixed point-to-point UNII devices operating in the 5.725 - 5.825 GHz band may employ transmitting antennas with directional gain up to 23 dBi without any corresponding reduction in the transmitter peak output power. For fixed, point-to-point UNII transmitters that employ a directional antenna gain greater than 23 dBi, a 1 dB reduction in peak transmitter power for each 1 dBi of antenna gain in excess of 23 dBi is required. Notice that by having an output power maximum of 30 dBm at the intentional radiator, and having a maximum of 23 dBi antenna gain before any reduction in transmitter output power is required, this allows these 5 GHz UNII systems to have an output of 200 Watts EIRP.



EIRP = 200 watts

$= 10\log 10^2 + 10.\log 2$

$= 10.2 + 3dBm$

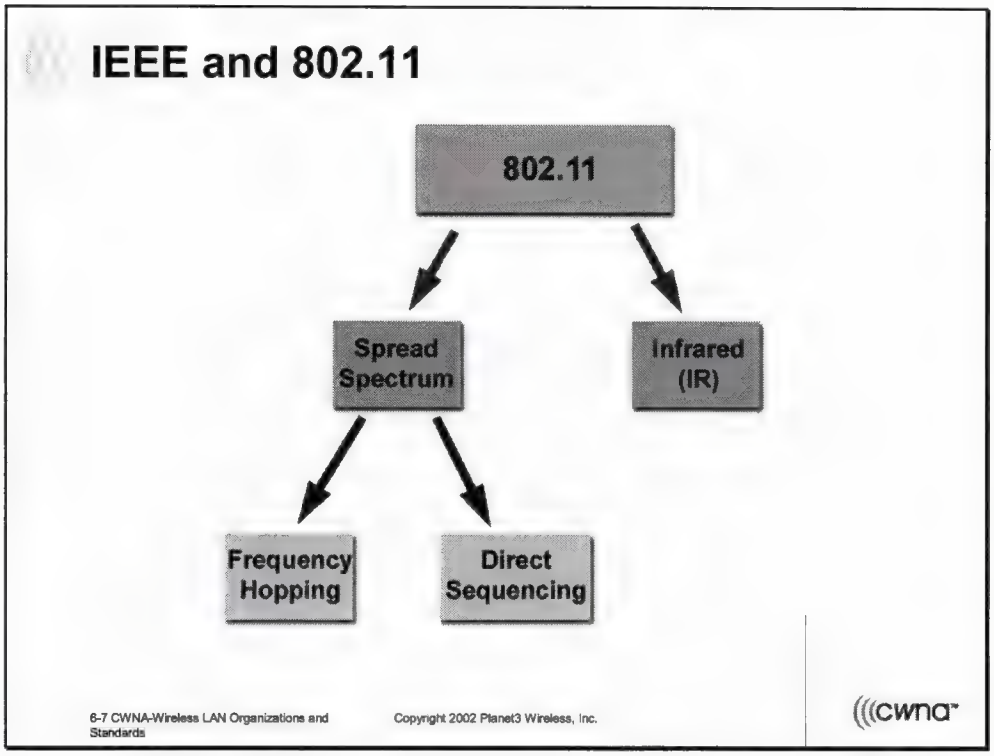
$= (20+3)\ DBm$

point-to-~~point~~ multipoint for 5GHz ONLY.

EIRP = 30 + 23 = 53 dBm

10 = 10
10 = 100
10 = 1000
10 = 10000
10 = 100000
3 = 200000 mW = 200 W

Copyright © 2003, Planet3 Wireless, Inc.



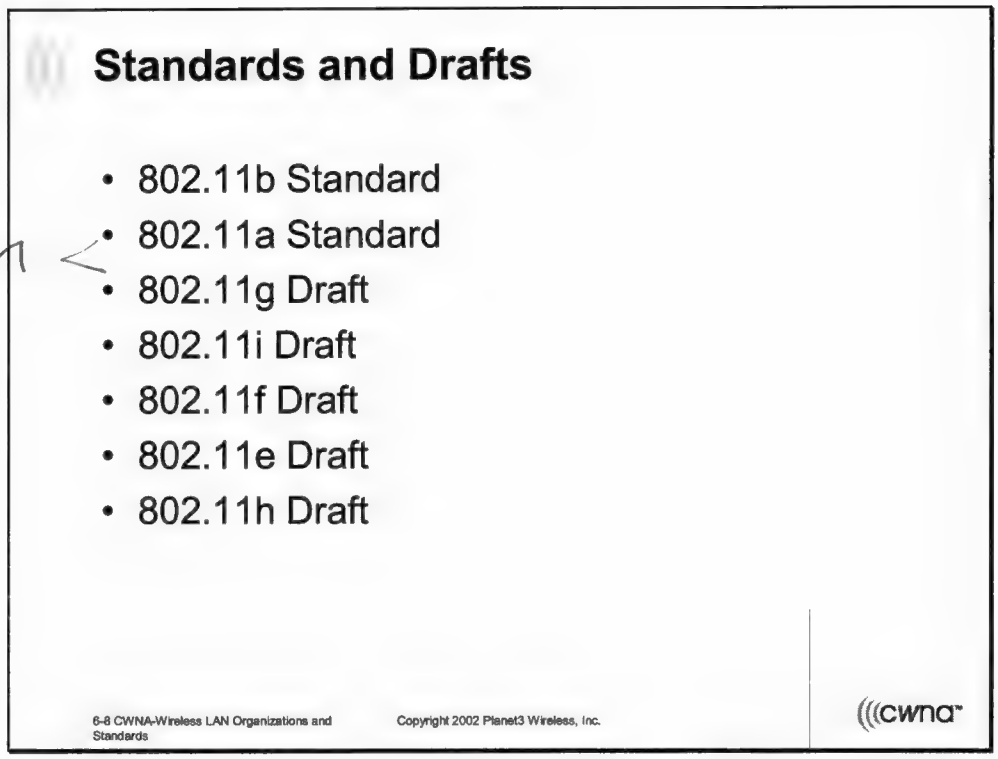
IEEE and 802.11

The IEEE 802.11 standard specifies use of both spread spectrum and infrared. Spread spectrum is further broken down into two components - frequency hopping (FHSS) and direct sequence (DSSS). The 802.11 standard, as specified by the IEEE, covers FHSS, DSSS, and infrared at 1 Mbps and 2 Mbps, although higher speeds are supported with each of these technologies.

The IEEE applies the FCC regulations for the 2.4GHz band to the 802.11 standards. For the 5 GHz UNII bands, the IEEE makes special output rules that are less than those which are specified by the FCC:

- Lower Band – 40 mW (5.15 – 5.25 GHz)
- Middle Band – 200 mW (5.25 – 5.35 GHz)
- Upper Band – 800 mW (5.725 - 5.825 GHz)

Copyright © 2003, Planet3 Wireless, Inc.



Standards and Drafts

The following standards and drafts are all based on the original 802.11 standard.

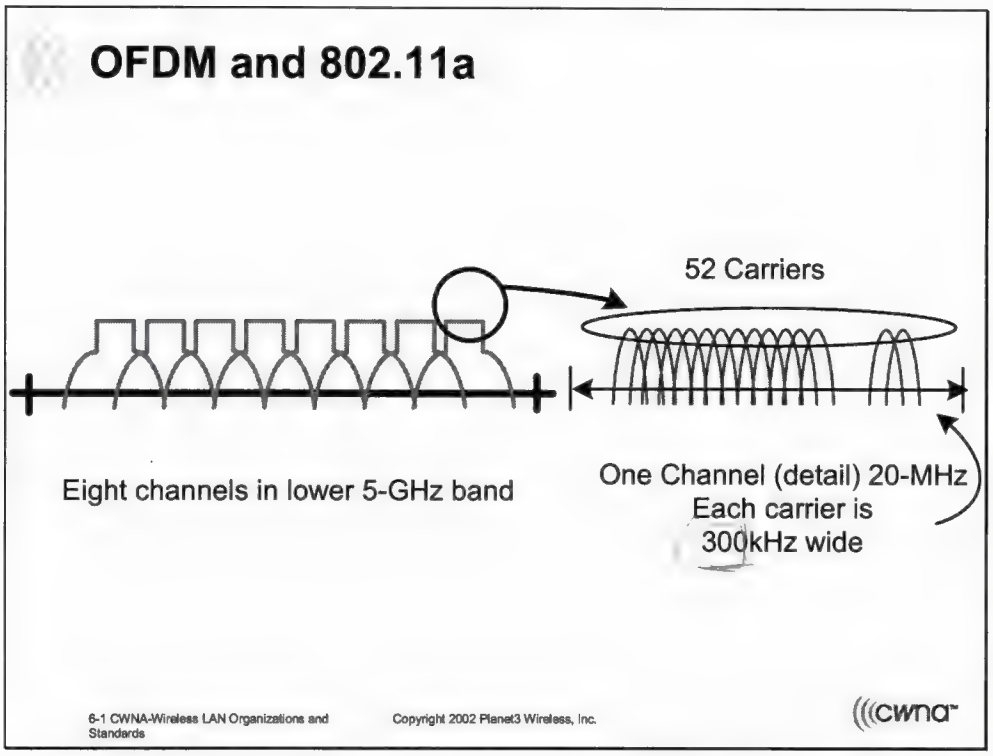
802.11b Standard

802.11b is a revision to the IEEE standard for direct sequence spread spectrum wireless LANs. 802.11b products have data rates of up to 11 Mbps.

802.11b covers only DSSS at 11 Mbps and 5.5 Mbps (backwards compatible with 802.11 using DSSS at 1 & 2 Mbps). This standard is very popular due to the good throughput and low cost of the components that are compliant with this standard.

The only difference between the 5.5 & 11 Mbps and the 1 & 2 Mbps data rates is the modulation techniques and spreading codes used. Instead of barker code with BPSK and QPSK modulation, 802.11b compliant products use complementary code keying (CCK) with QPSK modulation.

The 802.11b standard specifies use of the 2.4 GHz ISM band, as does the original 802.11 standard. The IEEE defines channels for use in this band that operate within the frequencies allotted by the FCC within the United States. The IEEE also defines channels for operation in other countries that work within those countries' frequency allocations.



802.11a Standard

802.11a is a revision to the IEEE standard that operates in the unlicensed 5 GHz band. Most 802.11a products support data rates up to 54 Mbps. The 802.11a standard specifies the use of UNII bands and the use of OFDM (Orthogonal Frequency Division Multiplexing) technology. This standard consists of 4 channels of 20 MHz with 5 MHz of separation between channels. There are a total of 12 non-overlapping channels – 4 channels each for the lower, middle, and upper bands.

OFDM is the secret behind how 802.11a gets up to 54 Mbps data rates. OFDM creates eight non-overlapping channels 20 MHz wide across the two lower bands of the 5 GHz UNII band (four channels in each of the two lower bands). Each of these eight channels is subdivided into 52 subcarriers, each approximately 300 KHz wide. Each subcarrier is transmitted in parallel, meaning that they are sent and receive simultaneously. A receiving station then processes these 52 incoming signals, each one representing a fraction of the total data transmitted, and makes up the complete transmission.

Due to the large amount of information being transmitted at such high rates, some means of error correction was required to prevent data loss. As such, Forward Error Correction (FEC) was added to IEEE 802.11a. FEC essentially sends two copies of the information in each transmission, a primary and secondary. If the primary transmission is damaged en route, the receiving station can recreate the lost data by running the secondary transmission through a set of algorithms. The performance impact is fairly negligible due to the high data rate.

Copyright © 2003, Planet3 Wireless, Inc.

The 802.11a standard requires speeds of 6, 12, and 24 Mbps, with a maximum of 54 Mbps. Typically manufacturer implementations include 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Any data rates higher than 54 Mbps use proprietary technology.

The Wi-Fi Alliance has announced that the Wi-Fi certification now also covers interoperable 802.11a products. They have further discussed that Wi-Fi for 802.11a will likely be geared to have 802.11h replace 802.11a in interoperability testing in the near future.

Due to the competing use of the 5 GHZ UNII bands by both 802.11a and HperLAN/2, 802.11a is not certified for usage in Europe as of yet by the ETSI. In an effort to solve this problem, two new additions have been proposed for the 802.11a standard: Dynamic Channel Selection (DCS) and Transmit Power Control (TPC). Together, these two solutions allow clients to detect the most available channels for use and then use the minimum amount of transmit power that is necessary if any interference is evident. With these additions, 802.11a may be licensed for use in Europe by ETSI as a short-time solution until the 802.11h standard is ratified by IEEE.

802.11h Draft

Both 802.11a and 802.11h are nearly identical, except that 802.11h includes Transmit Power Control (TPC) and Dynamic Channel Selection (DFS) from the beginning. This should allow 802.11a to become licensed in Europe very quickly once the final standard is ratified by the IEEE.

The Wi-Fi Alliance's Wi-Fi currently covers 802.11a, but not 802.11h just yet. Adding to the confusion, 802.11h is likely to replace 802.11a within the industry and the Wi-Fi brand. The 802.11h standard is backward compatible with 802.11a, but it is likely that 802.11a products bought in the U.S. won't work with European 802.11h access points. In Europe, access points could be set up to not accept connections from 802.11a devices, and that could be a regulatory requirement. The HiperLAN2 and 802.11 standards have nearly identical physical layers but are very different at the Media Access Control level, so the products aren't interoperable. 802.11 is true wireless Ethernet, while HiperLAN/2 on a technical level is more like wireless Asynchronous Transfer Mode. Products based on the two standards should be able to operate in the same room without causing interference. HiperLAN/2 and 802.11h will face off in the European market, since HiperLAN/2 products aren't expected to appear on the U.S. market anytime soon. While HiperLAN/2 is touted for its ability to guarantee specific bandwidth to specific users, there are quality-of-service standards being developed for 802.11 such as 802.11e.

802.11g Draft

The 802.11g draft uses the 2.4GHz band, the same one as used by 802.11b and 802.11. The fastest data rate specified by the 802.11g draft is 54 Mbps, the same as provided by 802.11a. To achieve the increased speed, OFDM technology is used at speeds higher than 11 Mbps. OFDM is the same coding technique used in 802.11a devices. For backwards compatibility at lower speeds, DSSS modulation and spreading code techniques match 802.11b and 802.11 standards.

Copyright © 2003, Planet3 Wireless, Inc.

The biggest disadvantage of 802.11g is that it resides in the crowded 2.4 GHz ISM band. Equipment that complies with the new 802.11g standard will likely overcrowd the 2.4 GHz band. The biggest advantage of 802.11g is its backward compatibility with 802.11b products. This backward compatibility could amount to substantial savings to a large enterprise that already has a large investment in 802.11b products.

802.11i Draft

802.11i will provide an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1x forms a key part of 802.11i along with EAP and per-session key distribution. Security is a major weakness of wireless LANs. Vendors have not improved matters by shipping products without setting default security features. In addition, the WEP algorithm weaknesses have been exposed. The 802.11i specification is part of a set of security features that should address and overcome these issues. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (Advanced Encryption Standard) and TKIP backwards compatibility. The Wi-Fi Alliance has announced that the Wi-Fi™ certification will support 802.11i.

802.11f Draft

The purpose of the 802.11f draft is the Inter-Access Point Protocol. This protocol provides inter-vendor roaming by allowing access points to communicate in a standard method.

802.11e Draft

The purpose of the 802.11e draft is to enhance 802.11 Medium Access Control to add Quality of Service (QoS) and other protocol improvements. Security enhancements were moved from this group to 802.11i. Suggested QoS functions are E-DCF and HCF. E-DCF is based on priority queues while HCF is based on a central controller. 802.11e also addresses multicast issues such as multicast group management and multicast acknowledgement.

Copyright © 2003, Planet3 Wireless, Inc.

Summary of IEEE Wireless LAN Standards

	802.11	802.11a	802.11b	802.11g
Frequency	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz
Data Rate(s)	1, 2 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	5.5, 11 Mbps	6, 9, 12, 24, 36, 48, 54 Mbps
Modulation	FHSS, DSSS	OFDM	DSSS	OFDM
Effective Data Throughput	1.2 Mbps	32 Mbps	5 Mbps	32 Mbps
Advertised Range	300 feet	225 feet	300 feet	300 feet
Encryption Available?	Yes	Yes	Yes	Yes
Encryption Type	40-bit RC4	40-bit, 104-bit RC4	40-bit, 104-bit RC4	40-bit, 104-bit RC4
Provides Authentication?	No	No	No	No
Network Support	Ethernet (IEEE 802.3)	Ethernet (IEEE 802.3)	Ethernet (IEEE 802.3)	Ethernet (IEEE 802.3)

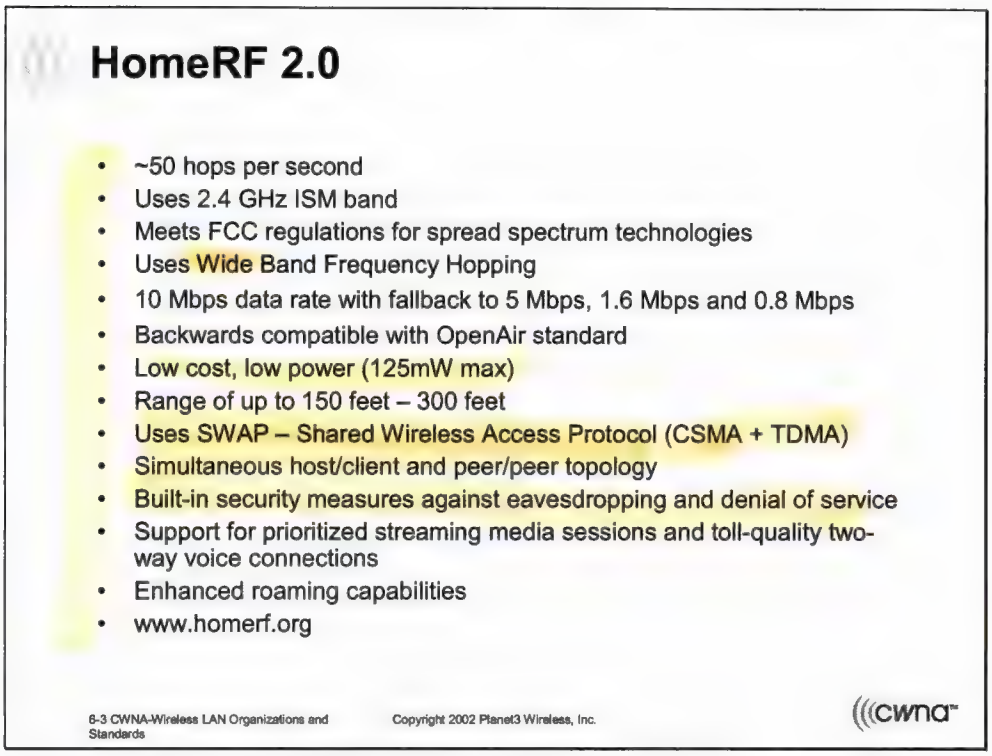
6-2 CWNA-Wireless LAN Organizations and Standards

Copyright 2002 Planet3 Wireless, Inc.

((cwna

Summary of IEEE Wireless LAN Standards

Its worth pointing out that the effective data throughput of all standards is usually about 50-60% of the maximum rated throughput. This is due to the nature of radio transmissions using half-duplex communications. As well, the advertised ranges are wildly variable and can be affected by all manner of obstructions. When we discuss site surveys later, you will get an idea what types of obstructions and interfering devices you will need to be aware of.


HomeRF 2.0
~50 hops per second
Uses 2.4 GHz ISM band
Meets FCC regulations for spread spectrum technologies
Uses Wide Band Frequency Hopping
10 Mbps data rate with fallback to 5 Mbps, 1.6 Mbps and 0.8 Mbps
Backwards compatible with OpenAir standard
Low cost, low power (125mW max)
Range of up to 150 feet – 300 feet
Uses SWAP – Shared Wireless Access Protocol (CSMA + TDMA)
Simultaneous host/client and peer/peer topology
Built-in security measures against eavesdropping and denial of service
Support for prioritized streaming media sessions and toll-quality two-way voice connections
Enhanced roaming capabilities
www.homerf.org
6-3 CWNA-Wireless LAN Organizations and Standards
Copyright 2002 Planet3 Wireless, Inc.
cwna

HomeRF

HomeRF was founded in March of 1998. This organization's charter is to establish the mass deployment of interoperable wireless networking access devices. HomeRF products utilize the 2.4 GHz ISM band, FHSS technology, and *Shared Wireless Access Protocol* (SWAP) to achieve data rates of up to 10 Mbps. HomeRF 2.0 is backward compatible with the OpenAir standard created by the WLIF, which supports speeds of 1.6 Mbps and 800 kbps. The HomeRF 2.0 standard (which uses post 8/31/00 rules on FHSS) supports 5 Mbps and 10 Mbps rates. HomeRF 2.0 has been cleared for European use by ETSI.

HomeRF technology hops at approximately 50 hops per second. A standard frequency hopping system in 802.11 would use 5-10 hops per second. Depending on the implementation of frequency hopping, HomeRF would be 5-10 times faster than 802.11. HomeRF is limited to a maximum output power of 125mW, which results in relatively short-range signal transmission. The maximum range of HomeRF is between 150 feet and 300 feet, depending on obstructions. Because this limits its effective use in enterprise markets, the intended market is typically the SOHO user.

HomeRF supports a QoS for voice and video using SWAP. The SWAP protocol is a mixture of CSMA (Carrier Sense Multiple Access) and TDMA (Time Division Multiple-Access).

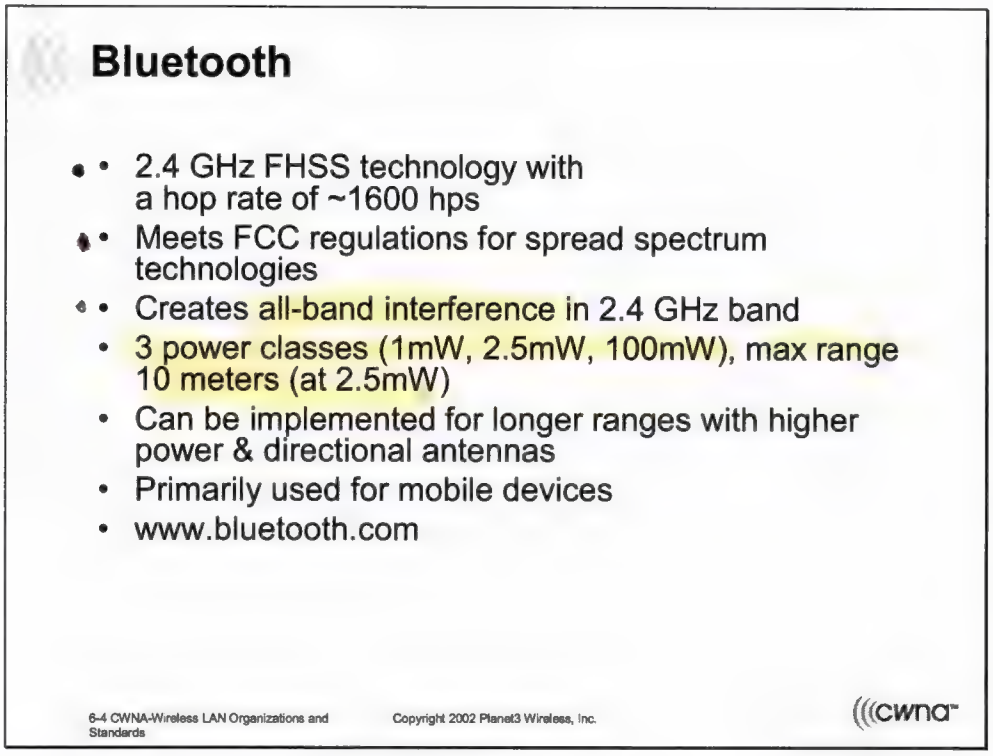
HomeRF 2.0 supports simultaneous host/client and peer/peer topology, power savings modes, and security measures against eavesdropping and denial of service.

Copyright © 2003, Planet3 Wireless, Inc.

Additionally, HomeRF 2.0 supports up to 8 simultaneous prioritized streaming media sessions for audio, video – either one-way or two-way – and up to 8 simultaneous toll-quality two-way cordless voice connections on up to 4 handsets. HomeRF 2.0 also has enhanced roaming capabilities including mobile initiated handoffs, seamless handoffs between adjacent or co-located access points, and peer-to-peer data transfers between roaming devices.

Note Proxim is currently the only manufacturer supporting HomeRF 2.0.

Copyright © 2003, Planet3 Wireless, Inc.


Bluetooth
2.4 GHz FHSS technology with a hop rate of ~1600 hps
Meets FCC regulations for spread spectrum technologies
Creates all-band interference in 2.4 GHz band
3 power classes (1mW, 2.5mW, 100mW), max range 10 meters (at 2.5mW)
Can be implemented for longer ranges with higher power & directional antennas
Primarily used for mobile devices
www.bluetooth.com
6-4 CWNA-Wireless LAN Organizations and Standards
Copyright 2002 Planet3 Wireless, Inc.
cwna

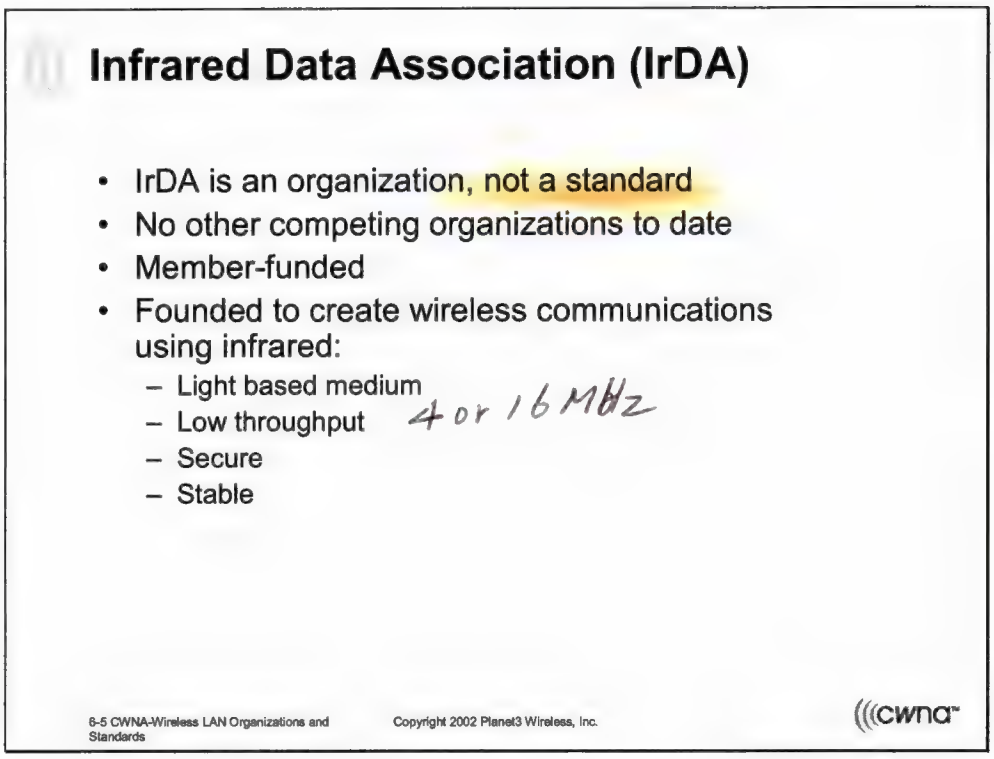
Bluetooth

Bluetooth is part of the 802.15 standard for WPANs (Wireless Personal Area Networks). Bluetooth is a close-range networking protocol primarily used for mobile devices, utilizing FHSS in the 2.4 GHz ISM band at around 1600 hops per second.

Because of the high hop rate, Bluetooth devices can greatly interfere with other devices operating in the 2.4 GHz band, including devices on 802.11, 802.11b, and HomeRF networks. The interference increases as Bluetooth devices are moved closer to wireless LANs.

There are solutions on the market that try to attempt to circumvent the interference issues between Bluetooth and 802.11 networking products. One client-side solution switches the services on and off to try to avoid the interference between the two. Adaptive Bluetooth attempts to locate which frequencies are being used by the 802.11 network and avoid transmitting on those frequencies. However, in the case where a wireless network has 3 access points co-located and direct sequencing is being used, Bluetooth does not have enough frequency space on which to transmit.

Copyright © 2003, Planet3 Wireless, Inc.


Infrared Data Association (IrDA)
• IrDA is an organization, not a standard
• No other competing organizations to date
• Member-funded
• Founded to create wireless communications using infrared:
– Light based medium
– Low throughput
– Secure
– Stable
4 or 16 MHz
6-5 CWNA-Wireless LAN Organizations and Standards
Copyright 2002 Planet3 Wireless, Inc.
cwna

Infrared Data Association

The Infrared Data Association (IrDA) was founded in June 1993. This organization's charter is to create an interoperable, low-cost, low-power, half-duplex, serial data interconnection standard that supports a walk-up point-to-point user model that is adaptable to a wide range of computer devices utilizing infrared light.

Infrared

Infrared is a light-based transmission technology. Infrared does not use spread spectrum RF. There are two types of infrared used in wireless LANs:

- Broadcast – used indoors mainly for PDAs and laptops
- Point-to-point – used outdoors

Throughput

The maximum speed of infrared is 4 Mbps. This throughput is twice that of the 802.11 standard, though it is normally implemented at 115 kbps, which is good for exchanging data on hand-held devices and laptop computers.

In a point-to-point application, infrared can achieve distances of up to 1 km. 802.11 compliant infrared devices can only use speeds of 1 & 2 Mbps although higher rates may be achievable with the proper equipment.

Security

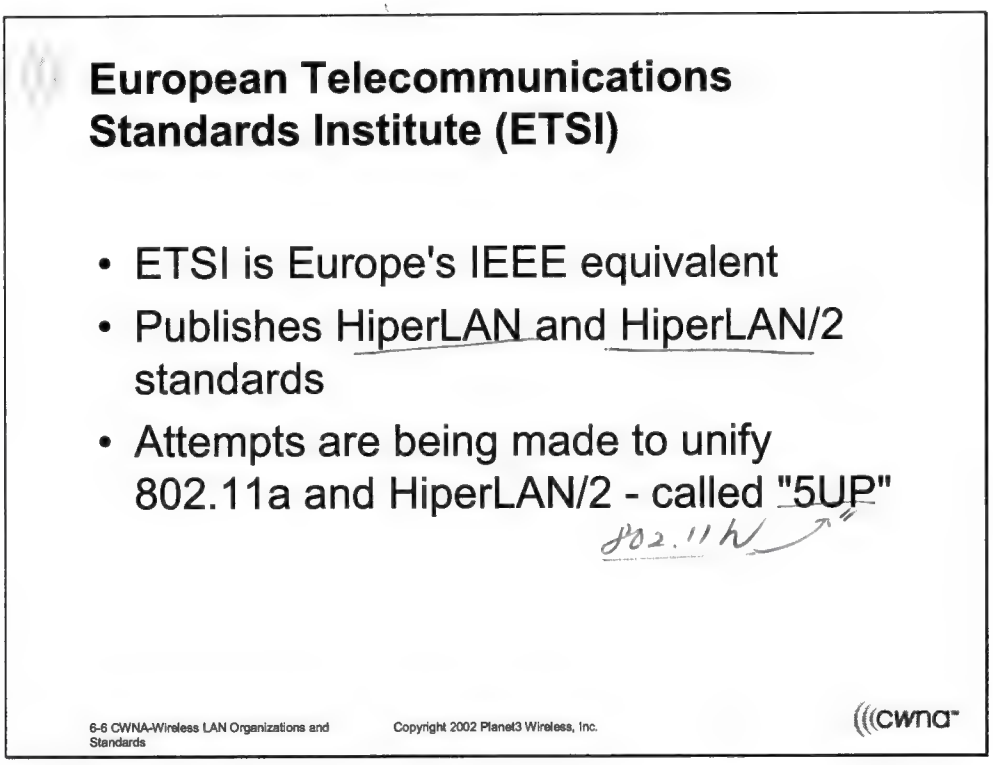
Infrared will not pass through walls and would-be hackers cannot eavesdrop without breaking the light beam. Both of these characteristics aid in security.

Stability

Infrared will bounce off of walls, which aids in single-room networking. Electromagnetic disruption does not affect the signal, which aids in stability.

What does affect the stability of the infrared beam is sunlight, which dilutes the signal. This dilution is caused by the sun's light, which is sixty percent infrared. Sunlight affects outdoor point-to-point infrared links and broadcast infrared when using computers to communicate outdoors in daytime.

Copyright © 2003, Planet3 Wireless, Inc.


European Telecommunications Standards Institute (ETSI)
• ETSI is Europe's IEEE equivalent
• Publishes HiperLAN and HiperLAN/2 standards
• Attempts are being made to unify 802.11a and HiperLAN/2 - called "5UP"
802.11h
6-6 CWNA-Wireless LAN Organizations and Standards
Copyright 2002 Planet3 Wireless, Inc.
cwna

European Telecommunications Standards Institute

The European Telecommunications Standards Institute (ETSI) is chartered with producing communications standards for Europe in the same way that the IEEE is for the United States. The standards ETSI has established, HiPerLAN/2 for example, directly compete against standards created by the IEEE such as 802.11a. There has been much discussion about IEEE and ETSI unifying on certain wireless technologies, but nothing has materialized yet. This effort is referred to as the "5UP" initiative for "5 GHz Unified Protocol."

ETSI's original HiPerLAN standard for wireless, dubbed HiperLAN/1, supported rates of up to 24 Mbps using DSSS technology with a range of approximately 150 feet. HiperLAN/1 used the lower and middle UNII bands, as do HiperLAN/2, 802.11a, and the new 802.11h draft. The new HiperLAN/2 standard supports rates of up to 54 Mbps and uses all three of the UNII bands. Additionally, HiperLAN/2 uses TDMA whereas IEEE's 802.11a uses CSMA/CA like the previous IEEE standards and drafts.

ETSI's HiperLAN/2 standard has interchangeable convergence layers, support for QoS, and supports DES and 3DES encryption. The supported convergence layers are ATM, Ethernet, PPP, FireWire, and 3G. Supported QoS awareness includes 802.1p, RSVP, and DiffServ-FC.

Chapter

7

802.11 Network Architecture

Objectives

Upon completion of this chapter you will be able to:

- Describe authentication and association and how they allow users to gain access to the wireless LAN
- Define the different types of service sets that can be configured
- Explain what beacons are and what information they provide
- Define the power management features available with wireless LANs
- Explain Dynamic Rate Shifting

7-2 CWNA-802.11 Network Architecture Copyright 2002 Planet3 Wireless, Inc. cwna™

Copyright © 2003, Planet3 Wireless, Inc.

Chapter Content

Part of an administrator's job tasks may be to choose a specific functionality of a wireless LAN over another solution, and to be able to discuss the available configurations that can be used within a wireless LAN with other administrators.

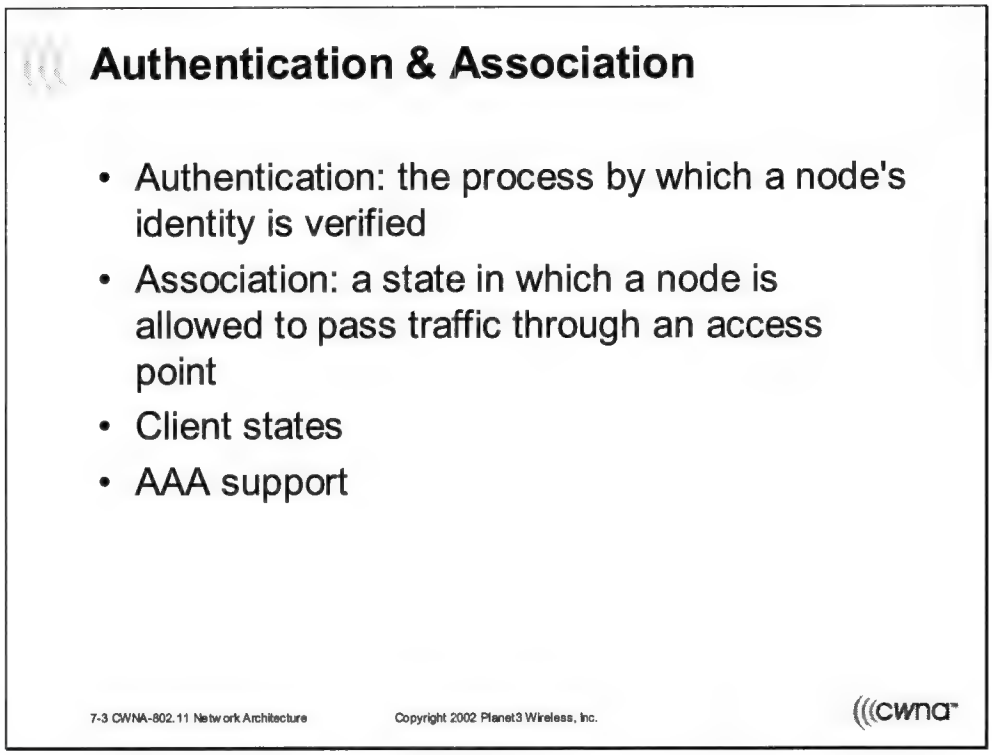
This chapter begins by explaining how client devices connect to a wireless LAN. Next, the different configurations of how wireless clients are grouped within the network are discussed. The available power management features for client devices and their differences are also explained.

The chapter outline follows:

- Authentication and Association
- Service Sets
- Beacons
- Power Management Modes
- Dynamic Rate Shifting

Copyright © 2003, Planet3 Wireless, Inc.

Authentication and Association


Authentication & Association
• Authentication: the process by which a node's identity is verified
• Association: a state in which a node is allowed to pass traffic through an access point
• Client states
• AAA support
7-3 CWNA-802.11 Network Architecture
Copyright 2002 Planet3 Wireless, Inc.
cwna

Authentication

Authentication is the process a station uses to announce its identity to another station. Authentication is the verification of identity and that the client is who he says he is. By the IEEE 802.11 standard, the process does not involve a great deal of checking; rather, the wireless client's identity is simply accepted.

The only case where a client's identity is not just accepted is when WEP or some other advanced security feature of a wireless LAN is used. The only authentication security feature specified by 802.11 is WEP. Other methods are available, but they are proprietary.

Association

Association is an IEEE 802.11 service that enables the mapping of a wireless station to the wired distribution system via an access point. The process of association is how a wireless client gets connected to the network. When a client is associated, it is connected to the network and able to pass traffic through the access point to which it is associated.

Access points generally have a configuration interface that allows the administrator to view which stations are associated at any particular time. Depending on the manufacturer, this interface may be custom software or a built-in web server.

Copyright © 2003, Planet3 Wireless, Inc.

Note The station indicates connectivity based on what type of client software the manufacturer provides. On a Windows 2000 machine for example, a connectivity program may be running in the system tray that indicates an active or broken connection.

Client States

A client can be in one of three states on the wireless LAN:

1. Unauthenticated & unassociated
2. Authenticated & unassociated
3. Authenticated & associated

Authentication occurs before association, and before the client can ever pass data through the access point. Authentication – verifying that a client is who it claims to be – must occur before the association process. If the client cannot be authenticated the access point ends the session. The client is then in an unauthenticated and unassociated state.

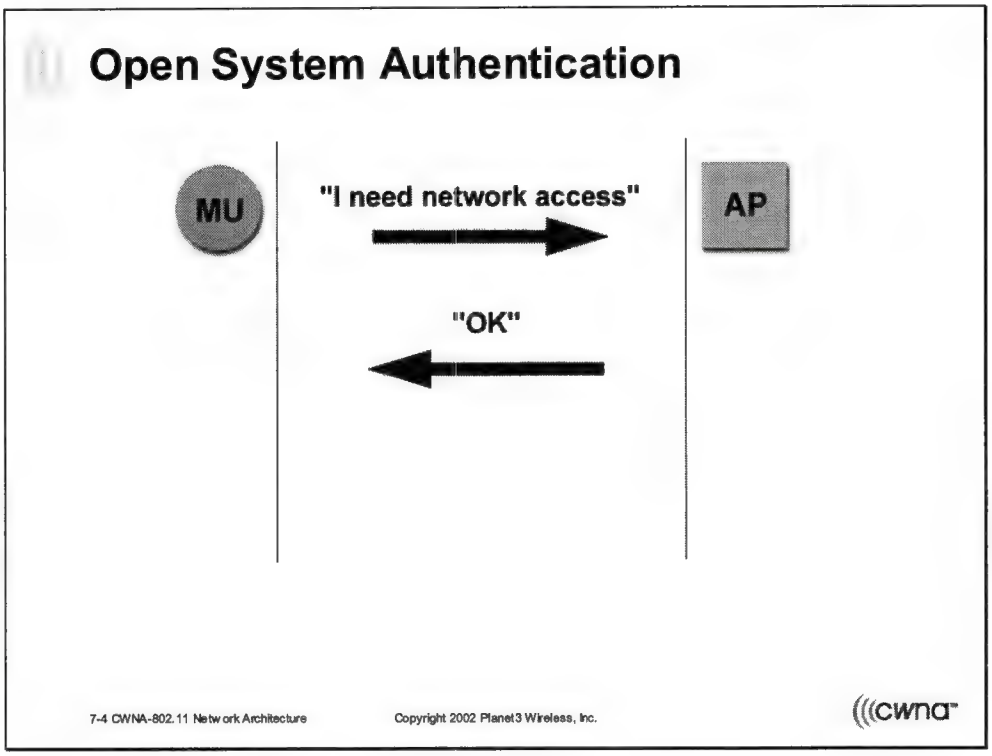
AAA Support

IEEE 802.11 does not specify any Authentication, Authorization, and Accounting (AAA) support. AAA implementation is left to the equipment manufacturers. Authentication is the verification of a station's identity. Authorization is a method of giving a station access to only the network resources necessary for that station. Accounting shows what a client has done and where they have been on the network.

Note It's important to note that mobile wireless clients can authenticate to more than one access point at a time, but may only associate with one access point. This pre-authentication makes for faster and smoother roaming when the client moves from the coverage area of one AP to another. You can verify clients pre-authenticating by checking the Association Table of your Access Points.

Copyright © 2003, Planet3 Wireless, Inc.

Authentication Process Types



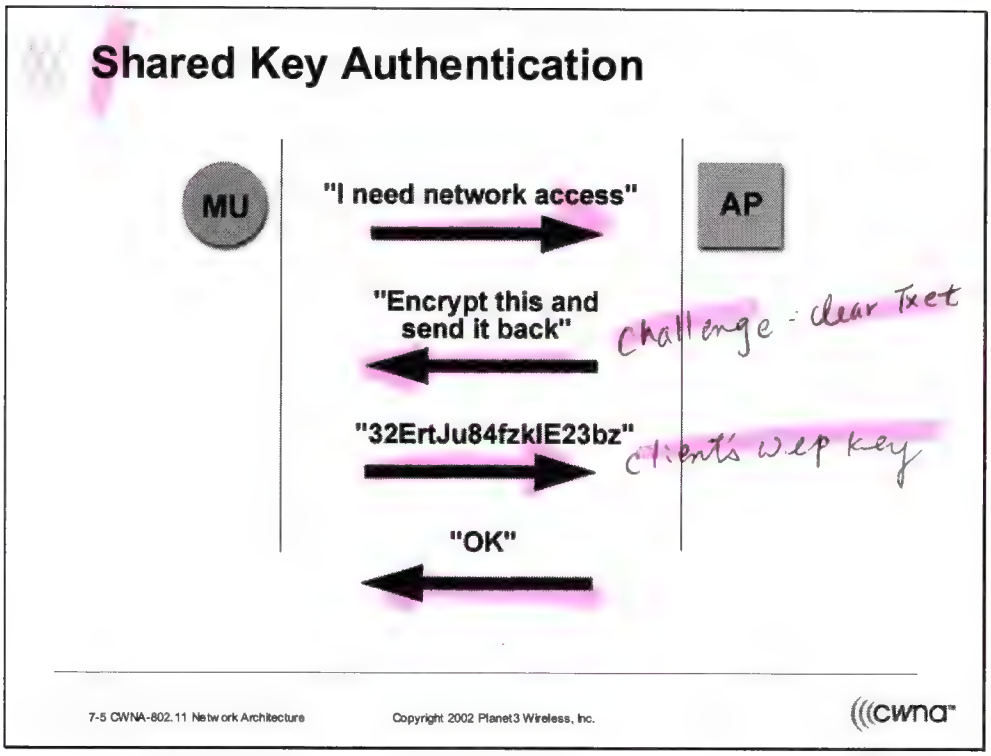
IEEE 802.11 specifies two processes of authentication: open system authentication and shared key authentication. An access point can support one or both authentication schemes, but at least one must be used since clients must associate in order to communicate.

Open System Authentication

Open system authentication is the IEEE 802.11 default authentication method. It consists of a very simple, two step process. First, the station wanting to associate to the network sends an association request frame to the access point. The access point then sends back an association response frame alerting the station as to whether it recognizes the identity of the authenticating station or not.

Using this method of authentication, a station can associate with any access point and listen to all data that is sent across that access point. If WEP is used with open system authentication, then the client is allowed to associate, but packets being passed between the access point and station are encrypted. If both units do not have the same encryption key, neither will understand anything the other is saying and the received packets are simply dropped.

Copyright © 2003, Planet3 Wireless, Inc.



Shared Key Authentication

Shared key authentication is a type of authentication that assumes each station has received a secret shared key through a secure channel independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of shared key authentication requires implementation of the 802.11 Wired Equivalent Privacy (WEP) algorithm. The WEP key resides in each station's radio card firmware in a write-only format. The steps to shared key authentication are:

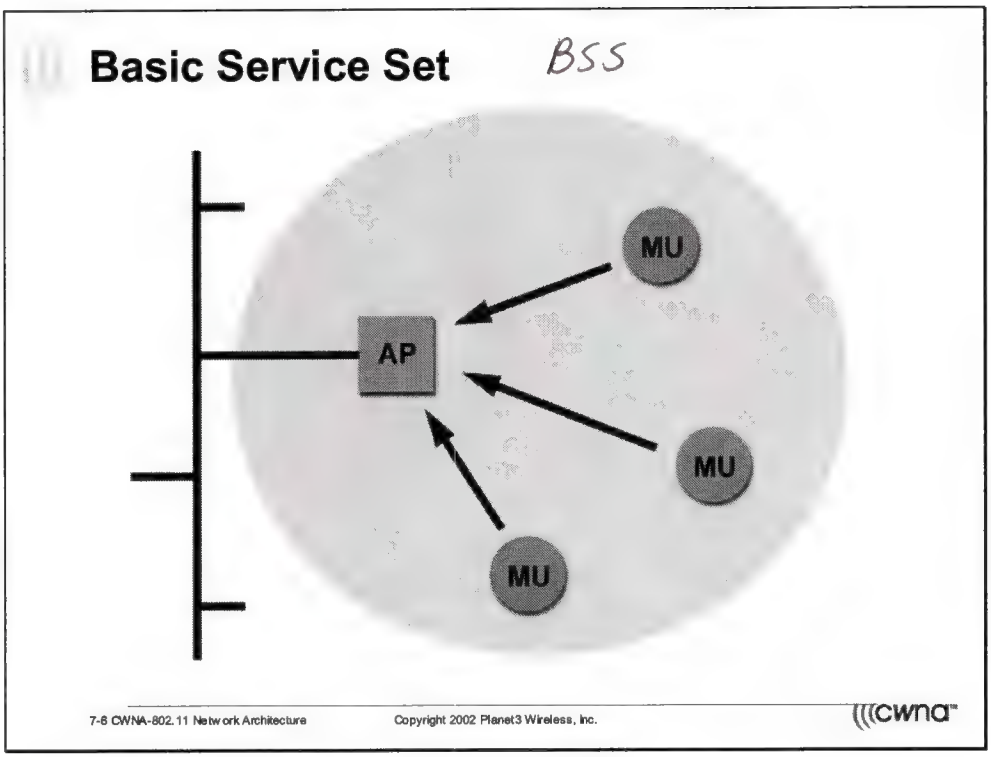
1. The client makes a request to associate by sending an association request frame.
2. The access point sends a clear text challenge to the client.
3. The client responds to the access point by sending back the challenge text encrypted using the client's WEP key.
4. The access point decrypts the challenge text with its own WEP key. If the access point sees that the challenge text and decrypted text are the same, the access point sends back an association response frame authenticating the client.

With shared key authentication, use of the WEP key is mandatory for authentication and encryption.

Note Because a hacker can collect the plain text and the encrypted response, the WEP key can be determined. This generally means that open system authentication is more secure than shared key authentication.

Copyright © 2003, Planet3 Wireless, Inc.

Service Sets

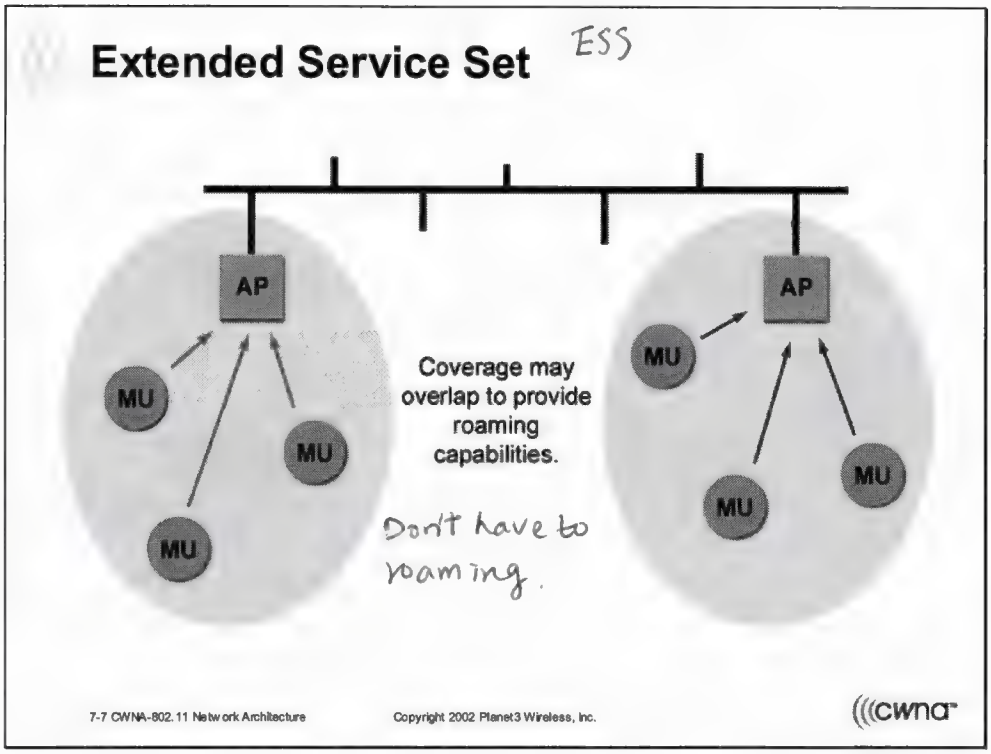


Basic Service Set

A basic service set (BSS) is a set of 802.11-compliant stations and an access point that operate as a fully connected wireless network. Use of a BSS is also commonly referred to as infrastructure mode. A basic service set uses a single cell and a single SSID (network name). A cell refers to the RF field around an access point. A BSS requires exactly one access point.

When using only one access point, the network is in infrastructure mode by default. In infrastructure mode, when one client sends data to another client, the data must go through the access point. In this mode, the access point acts as the gateway between the wireless LAN and the wired LAN segments.

Copyright © 2003, Planet3 Wireless, Inc.



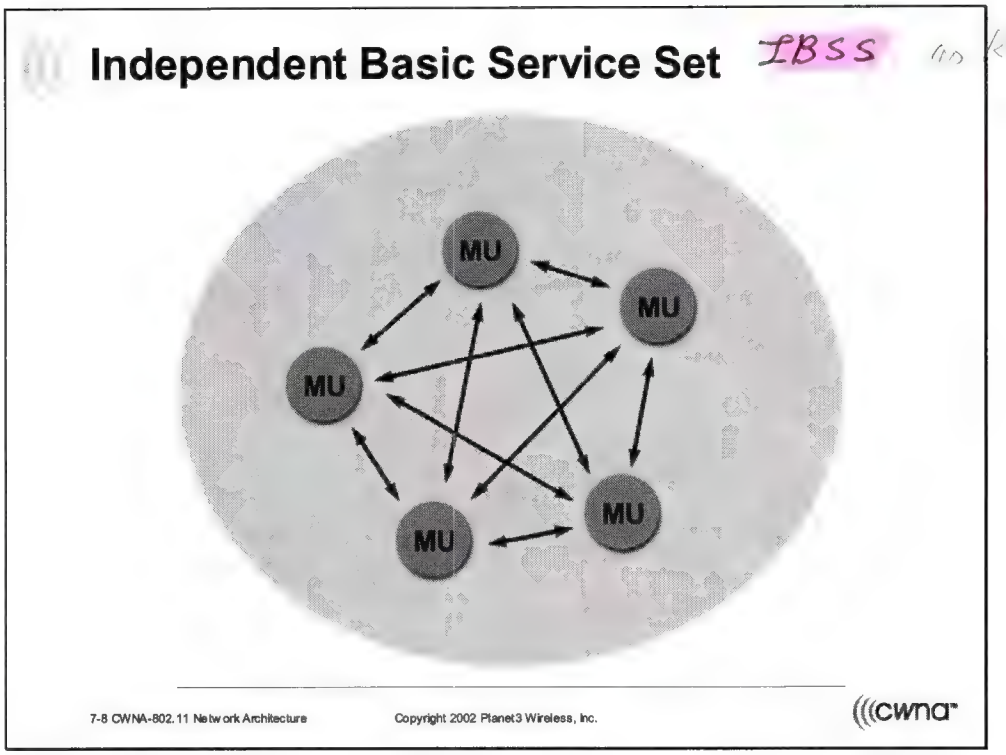
Extended Service Sets

The IEEE 802.11 standard defines an extended service set (ESS) as a collection of basic service sets tied together via a common distribution system such as Ethernet or Token Ring. An ESS, like a BSS, is also considered infrastructure mode. An ESS must have at least 2 access points, so that it consists of multiple cells.

The ESS does not have to support roaming, although roaming is allowed and sometimes required based on user needs. Roaming can be seamless or non-seamless depending on how the network is configured and the range of each the access point. When the cells of the access points overlap, users can roam from one cell to another without losing network connectivity.

The IEEE 802.11 standard does not specify that there must be roaming between two or more BSS that form an ESS. Thus, one cell could be running IPX and another could be running IP, and it would still be considered an ESS if the two nodes are connected by a common distribution system.

Copyright © 2003, Planet3 Wireless, Inc.

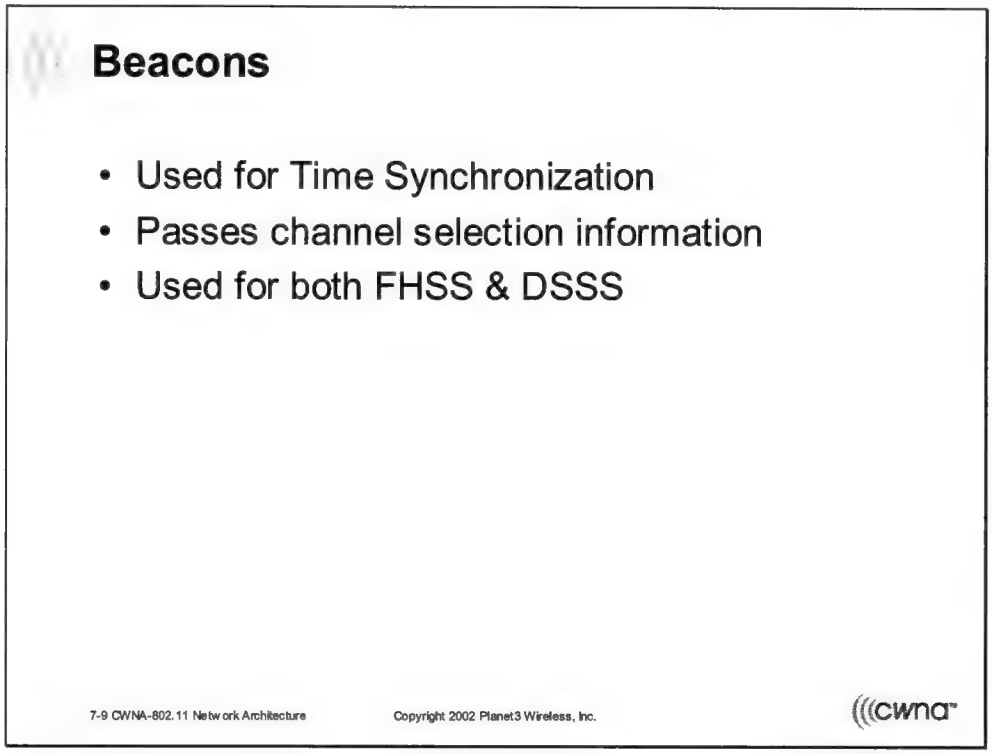


Independent Basic Service Set

An independent basic service set (IBSS) is an IEEE 802.11-based wireless network that has no backbone infrastructure and consists of at least two wireless stations and no access point.

This type of network is often referred to as an ad hoc network because it can be constructed quickly without much planning and has no access point with which to connect. Client stations connect directly to each other (peer-to-peer). An IBSS has a single cell and one SSID.

In ad hoc mode, one node must act as a gateway (router) in order to send packets out of the wireless LAN segment.


Beacons
• Used for Time Synchronization
• Passes channel selection information
• Used for both FHSS & DSSS
7-9 CWNA-802.11 Network Architecture
Copyright 2002 Planet3 Wireless, Inc.
cwna

Beacons

Beacons (short for "beacon management frame") are short frames sent from an access point to client devices for the purposes of:

- Time synchronization between the clients and the access point
- Passing channel selection information
- Informing clients of supported transmission rates
- Informing clients of DSSS or FHSS parameter sets
- Informing clients of capacity information
- Sending the Traffic Indication Map

Beacons are used by both FHSS and DSSS wireless LANs.

Time Synchronization

For certain features such as power saving mode, the access point and all clients must be time synchronized. When an access point sends a frame, the frame is time-stamped. When the client receives the frame, it reads the timestamp and updates its clock so that the client and access point stay synchronized. This process allows any client that is in a power saving mode to wake up at a specified interval to receive beacons.

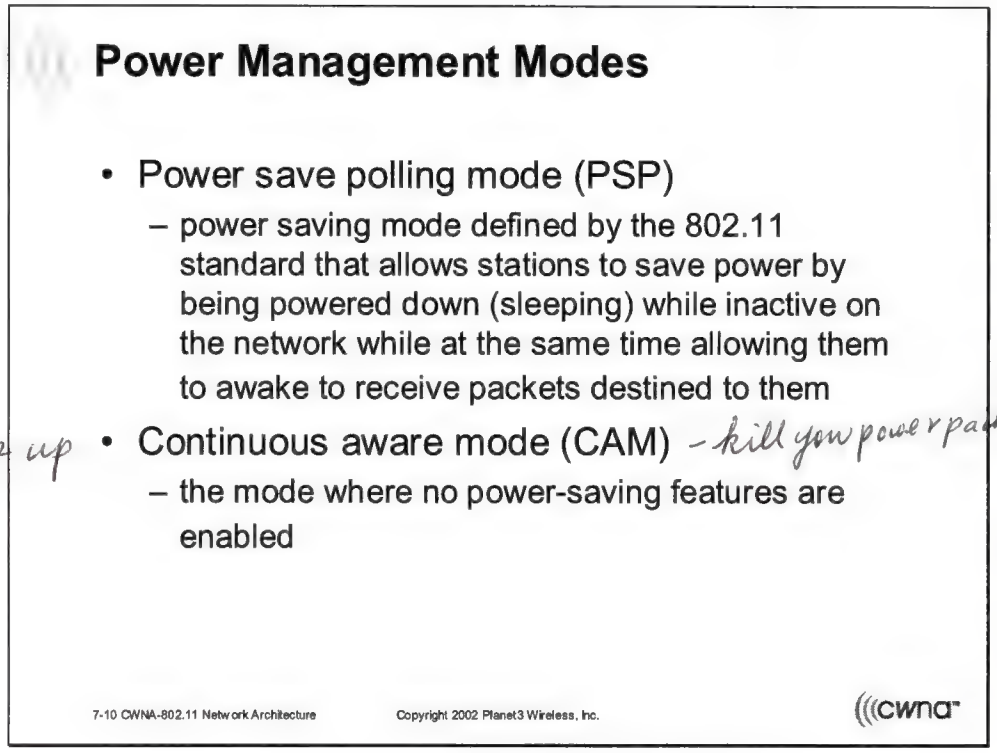
Copyright © 2003, Planet3 Wireless, Inc.

Channel Information, Parameter Sets, & Supported Rates

For FHSS, beacons will contain information about the frequency hopping sequence, current transmit frequency, and dwell time. Beacons transmitted using DSSS will contain the channel that is being used. Since there are many speeds of operation for wireless LANs, the beacons must pass transmission rate capability information. For example, an 802.11 access point will only announce support for 1 & 2 Mbps to clients whereas 802.11b access points will announce support for 11, 5.5, 2, & 1 Mbps support. Announcing supported rates lets the client know at what speeds it can connect with the access point.

Copyright © 2003, Planet3 Wireless, Inc.

Power Management Modes


Power Management Modes
• Power save polling mode (PSP)
– power saving mode defined by the 802.11 standard that allows stations to save power by being powered down (sleeping) while inactive on the network while at the same time allowing them to awake to receive packets destined to them
• Continuous aware mode (CAM)
– the mode where no power-saving features are enabled
7-10 CWNA-802.11 Network Architecture
Copyright 2002 Planet3 Wireless, Inc.
CWNA

Power Save Polling Mode

Power save polling mode (PSP), part of the 802.11 standard, allows the client to go to sleep instead of staying on all the time. This feature allows mobile units to conserve battery life, and to keep client devices cooler for longer component life.

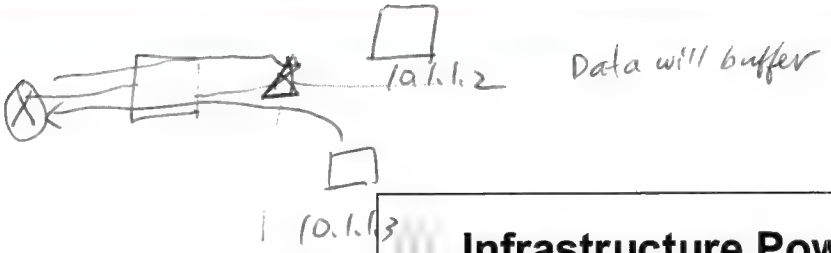
It is important to keep a perspective on how long a client goes to sleep. To an RF radio, seconds are years, and sleeping when saving power occurs in milliseconds. Clients may turn off and on several times per second. A client may use as little as 20 milliamps of power when sleeping.

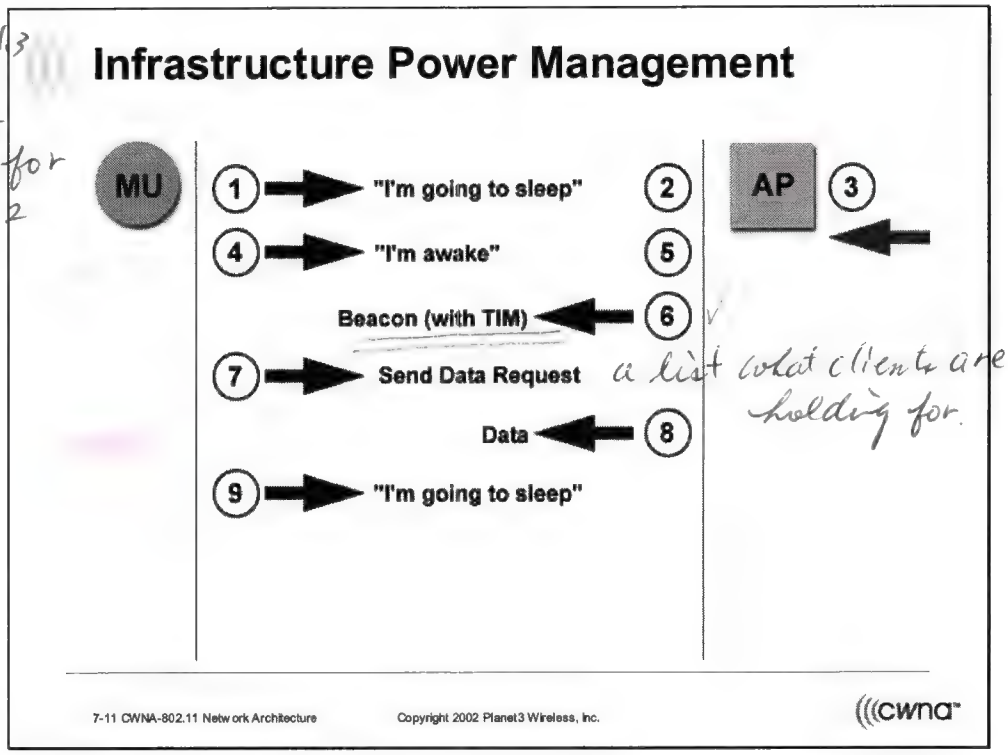
The PSP process relies on the time synchronization provided by beacons so clients can wake up at the correct interval.

Continuous Aware Mode

Continuous Aware Mode (CAM) is simply the absence of power saving functionality. If battery life were not an issue, such as for clients that have AC power, power saving would not be needed.

Copyright © 2003, Planet3 Wireless, Inc.



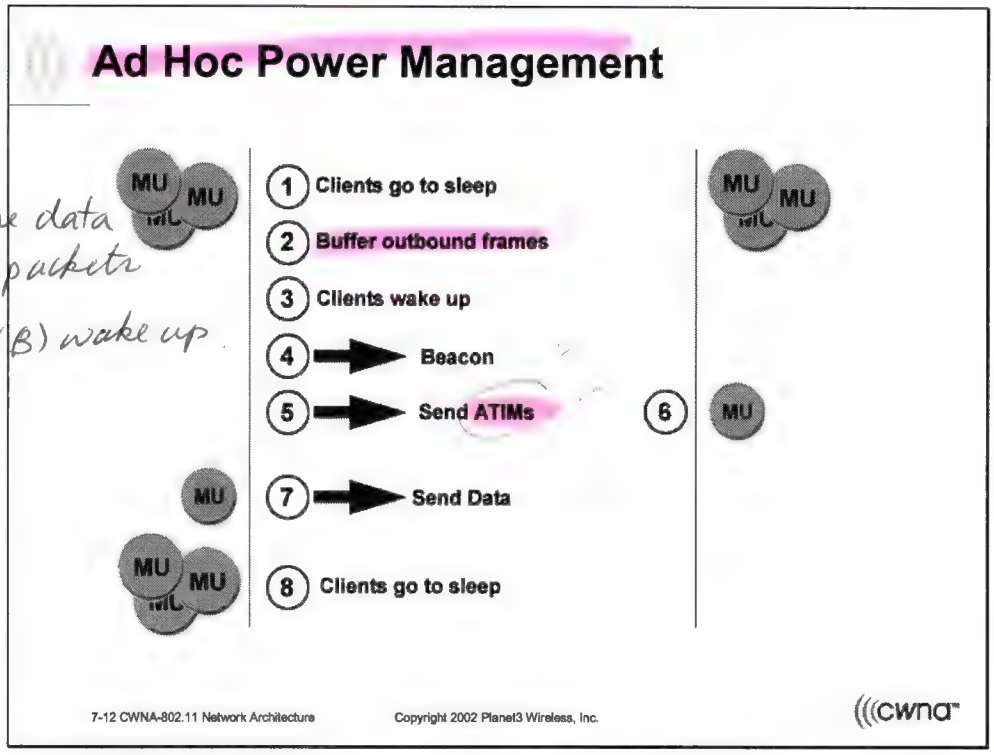


Infrastructure Mode Power Management

The following steps outline how PSP works in a BSS or ESS.

1. Each client configured for PSP informs the access point that it is going to sleep by toggling the power management bit in the frame control field of each MAC frame.
2. The access point receives these frames from the clients and keeps a table of every client that is sleeping.
3. Traffic comes into the access point destined for a sleeping client. The traffic cannot be sent to a sleeping client, so the access point buffers the data.
4. Each client configured for PSP awakes at a predetermined time and sends a frame to the access point notifying the access point that the client is awake.
5. The access point receives these frames from the clients and updates the table of which clients are sleeping.
6. The access point sends a beacon, which contains the traffic indication map (TIM). The TIM indicates which clients have frames buffered at the access point.
7. When the client sees that it has traffic buffered for it at the access point, the client sends a frame to the access point requesting that the buffered frames be sent.
8. The access point sends the buffered frames to the client
9. Each client configured for PSP informs the access point that the client is going to sleep again.

client sending the data will buffer the packets until the client(B) wake up



Ad Hoc Mode Power Management

With ad hoc power management, instead of using a TIM, an ATIM is used. ATIM stands for 'announcement traffic indication message'. The announcement traffic indication message is not a map, but rather a message (a unicast frame) that is transmitted from one station to another.

The ATIM notifies the receiving station to stay awake because there are frames buffered by another station destined to the receiving station. The ATIM is sent during a time window called an ATIM window. This period of time is when stations buffering frames destined to other stations can send ATIMs.

In ad hoc mode there is no central device for buffering frames, but rather each station must buffer frames for other stations to which it wants to send data. There is no announcement of sleep to any central device like there is in infrastructure mode. Stations sleep when there are no frames to be received and wake up in order to receive the beacon.

Ad hoc clients collectively handle beacon responsibilities, alternating between them which one sends the beacon. Beacons are used in the same fashion as in infrastructure mode where time stamping of frames keeps stations synchronized.

Copyright © 2003, Planet3 Wireless, Inc.

The following steps outline how the PSP process works in an IBSS.

1. Clients go to sleep when finished receiving data from other clients.
2. Clients buffer outbound frames.
3. Clients wake up.
4. The proper station sends the beacon.
5. Each station that is buffering frames to the destination clients sends an ATIM.
6. Clients receive ATIMs from one or more other clients and know to stay awake to receive the data.
7. The ATIM window closes and clients send and receive data.
8. Once a client receives the frames it was expecting per the ATIM, the client goes back to sleep.

Copyright © 2003, Planet3 Wireless, Inc.

Dynamic Rate Shifting

- Adaptive (or Automatic) Rate Selection (ARS) & Dynamic Rate Shifting (DRS) are both terms used for providing a method of speed fallback on a wireless LAN client as distance increases from the access point

7-13 CWNA-802.11 Network Architecture Copyright 2002 Planet3 Wireless, Inc. ((cwna

Dynamic Rate Shifting

The IEEE 802.11b standard defines dynamic rate shifting, allowing data rates to be automatically adjusted for noisy conditions or increased distance between the transmitter and receiver. This means IEEE 802.11b devices will transmit at lower speeds, 5.5 Mbps, 2 Mbps, and 1 Mps under noisy conditions, or as a mobile client moves farther and farther away from an access point. When the devices move back within close range of the access point, the connection will automatically speed up again. The speed selection decision is made based primarily on signal strength of the access point.

Dynamic rate shifting is required at 1, 2, 5.5, & 11 Mbps for wireless LAN devices to be 802.11b compliant. Both FHSS and DSSS implement DRS.

Dynamic rate shifting may also be referred to as Adaptive Rate Selection or Automatic Rate Selection (ARS).

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

8 MAC & Physical Layers

Objectives

Upon completion of this chapter you will be able to:

- Explain how a client joins a network
- Describe the modes of operation wireless LANs use to communicate
- Explain how wireless LANs avoid collisions on the network
- Define the Request-to-Send / Clear-to-Send transmission protocol
- Explain the effects of fragmentation on a network

8-2 CWNA-MAC & Physical Layers Copyright 2002 Planet3 Wireless, Inc. ((cwna™

Copyright © 2003, Planet3 Wireless, Inc.

Chapter Content

Wireless LANs communicate differently than Ethernet networks. There are different modes of communication and different ways to handle collisions. When installing, configuring, and troubleshooting wireless LANs, it is important to be aware of the lower level functions that are the foundation of wireless networking. This foundational knowledge will greatly assist administrators in certain aspects of administering a wireless LAN.

This chapter discusses some of the Physical and Data Link layer transmission protocols used in wireless LANs, including how collisions of network packets are handled. Also explained is how a client joins a network when the client is first powered on or enters a new cell.

The chapter outline follows:

- Joining a Network
- Communication Modes
- Collision Handling
- Request-to-Send/Clear-to-Send (RTS/CTS) Protocol
- Fragmentation

TIM- unicast
DTIM- multicast. /broadcast.

Copyright © 2003, Planet3 Wireless, Inc.

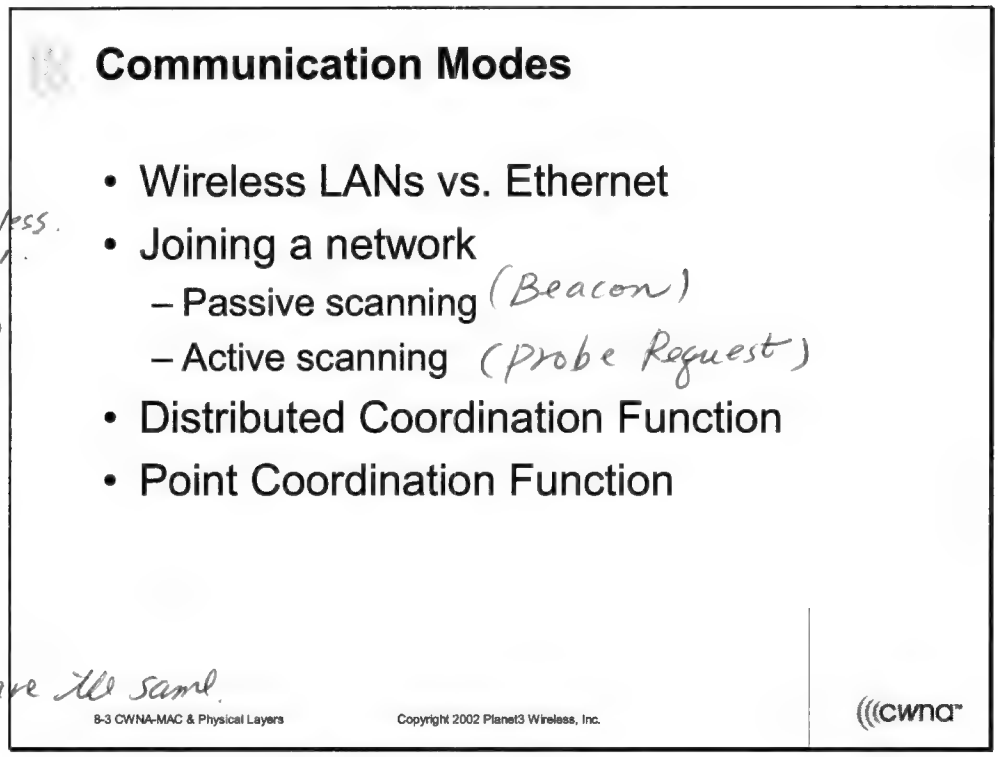
AiroPeek NX is good for Layer 2 above.

802.11 LSAP frame } can't
802.11 SNAP frame } see wireless 802.11.

802.3 LSAP ≠ 802.11 LSAP
802.3 SNAP ≠ 802.11 SNAP

have changed the structures of frames

Layer 3 (above) wire and wireless are the same.



Communication Modes

Wireless LANs vs. Ethernet

Wireless LANs do not use Ethernet frames to communicate, although the term "wireless Ethernet" may be used to describe them from time to time. Wireless LAN frames carry additional information including, among other things, sleep mode information, the channel being used, and the SSID (not an exhaustive list). In reality, there are actually three distinctly different types of wireless frames on the wireless LAN: control, management and data. Each of type of frame is constructed differently from the others and carries information related to its name.

Wireless LANs support all of the same layer 3 protocols as Ethernet such as IP, IPX, Decnet, and others.

Joining a Network

Scanning is the process by which clients determine whether a wireless network is present so that the client can join the network. Scanning occurs before authentication and association with an access point or an ad hoc network. Through passive or active scanning, the client will discover the other stations on the network.

Passive Scanning

Passive scanning is a method by which wireless clients keep a table of available access points or ad hoc networks by listening to beacon management frames. The table can be used later to identify other access points when the client is roaming. Generally clients will authenticate and associate with the access point that has beacon management frames with the strongest received signal strength. The process of keeping a table reduces the time it takes an end station to find another wireless network connection when roaming.

Active Scanning

Active scanning involves end stations broadcasting a probe frame. All access points within range of the end station respond with a probe response frame. The probe response frame from each access point includes almost identical information to that of a beacon. The signal strength of the probe response frames that the client receives is used to determine the access point to which the client will connect.

Distributed Coordination Function

Distributed Coordination Function (DCF) is an IEEE 802.11 mode of operation in which all stations desiring control of the transmission medium contend for access using the CSMA/CA protocol. CSMA/CA is similar to the 802.3 Ethernet protocol CSMA/CD in that it is a set of rules for accessing a shared medium.

DCF is the mode used when everyone on the network is arbitrating for use of the medium. The access points act like hubs to transmit the data, and DCF is the mode by which the data is transmitted.

Basic Service Sets (BSS), Extended Service Sets (ESS), and Independent Basic Service Sets (IBSS) can all use DCF mode.

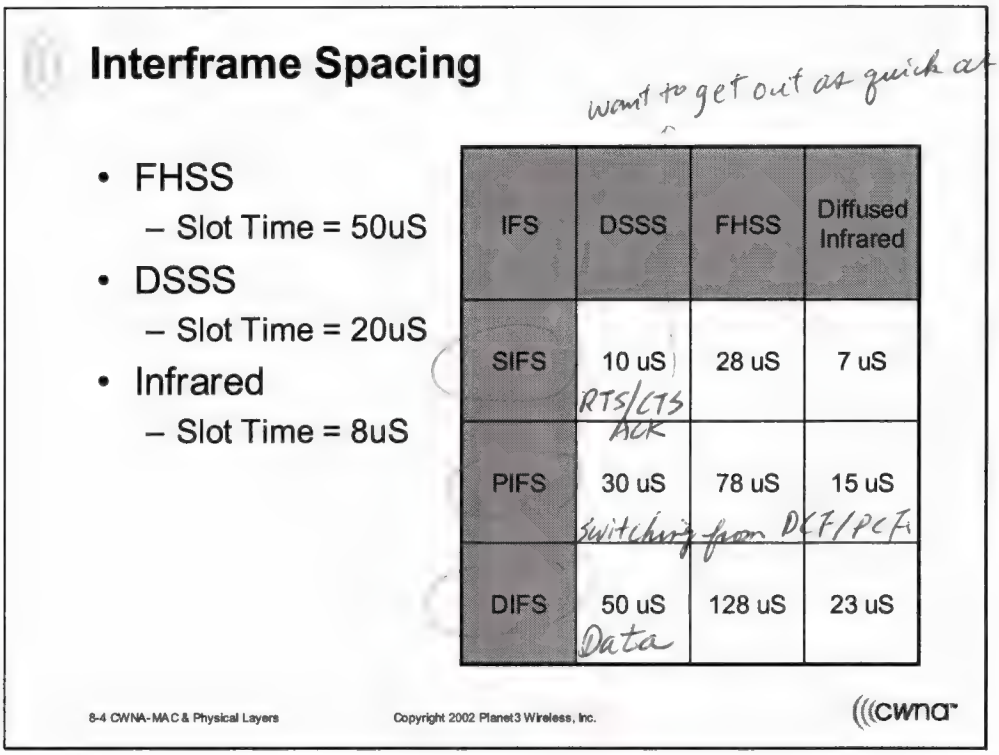
Point Coordination Function

Point Coordination Function (PCF) is an IEEE 802.11 mode that enables contention-free frame transfers based on a polling mechanism. Stations are polled for the need for frame transmission. The advantage to using PCF is that it provides a small amount of Quality of Service (QoS). PCF mode provides a given level of QoS for time-bounded services such as voice and video by guaranteeing latency. The disadvantage of using PCF mode is the additional overhead it adds resulting in lower throughput across the wireless LAN.

Basic Service Sets (BSS) and Extended Service Sets (ESS) can use PCF with DCF mode. PCF mode can never work without DCF.

Independent Basic Service Sets (IBSS) cannot use PCF mode because there is no device available to do the polling. An access point, which is not present in an ad hoc network, does polling.

Copyright © 2003, Planet3 Wireless, Inc.



Interframe Spacing

Interframe spacing is a way of collectively referring to a list of standard time spaces used in wireless LANs. To understand how interframe spacing is used, it is first important to understand the different types of spaces. The chart above shows the types of spaces and for which 802.11 technology they are used. Interframe spaces are measured in microseconds (uS).

SIFS - Short Interframe Space

PIFS - Point Coordination Function Interframe Space

DIFS - Distributed Coordination Function Interframe Space

EIFS - extended Interframe space

There is an EIFS (Extended Interframe Space), but discussion of how EIFS is used is beyond the scope of this text. The EIFS is only used when there are transmission errors, and its length is variable based on a given circumstance.

won't see those time intervals: SIFS, PIFS, DIFS, EIFS.

SIFS

SIFS are short in duration and are used when transmitting:

- RTS
- CTS
- ACK
- Polling ACK

This short duration space is used on the network when functions are required that only take a very short period of time to complete, like acknowledging receipt of a frame. Upon receiving an RTS, CTS, or ACK, a receiving station needs time to process the data and formulate a response to the sending station. The SIFS time period gives the receiving station to time to appropriately respond to a message.

PIFS

When polling stations, an access point uses PIFS. PIFS is used as a priority mechanism so that the access point may gain control over the medium before any contending stations. The PIFS space is shorter than the DIFS space (see chart) so that, if the access point only has to wait for PIFS to expire while stations are waiting for DIFS to expire, the access point will always be able to take control of the medium before the stations.

PCF mode is never used alone. PCF is always paired with DCF so that, after polling is complete, stations may continue to contend for network access.

When using polling, a period of time called a "superframe" is used to keep the access point from dominating the medium. The superframe (also referred to as the CFP Repetition Interval) is a period of time that is divided into two parts:

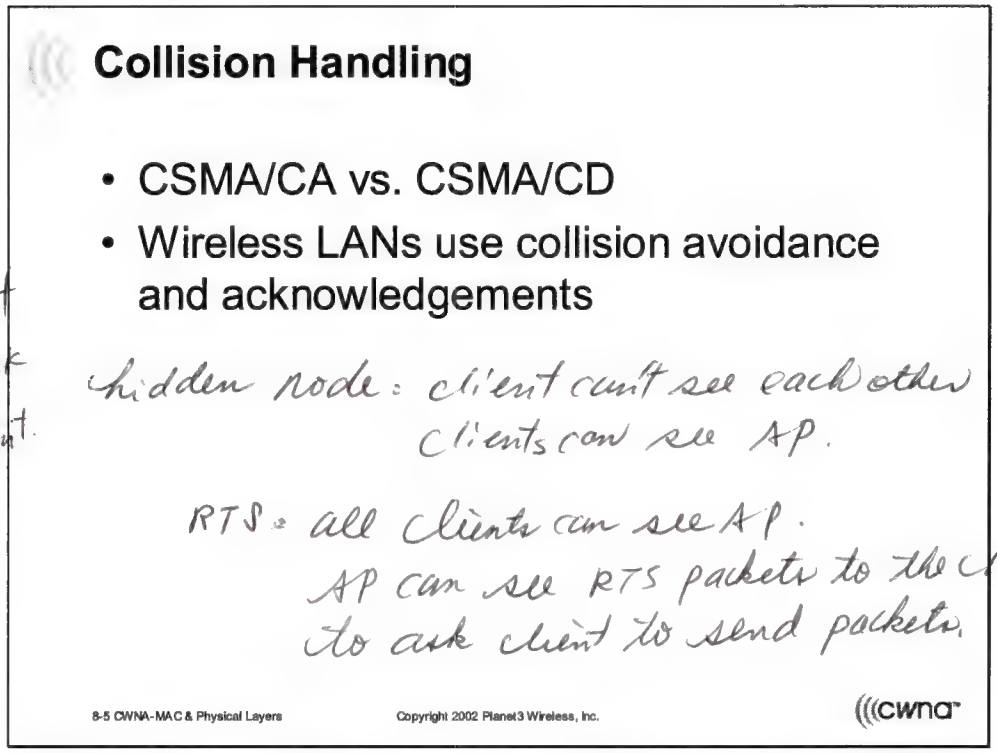
- Contention Free Period (CFP) - this also includes the Beacon management frame
- Contention Period (CP)

The CFP is the period of time within the superframe when the access point is allowed to poll stations. A beacon is sent by the access point (the Point Coordinator) at the beginning of each CFP that has the Network Allocation Vector (NAV) set to a value sufficient to keep all stations quiet until the predetermined end of the CFP. At the end of the CFP (which is the beginning of the CP) stations are allowed to contend for network access and the access point is not allowed to poll stations. The end of a CFP is announced by the access point with a CF-End frame.

DIFS

DIFS is used both by access points (during any contention period) and by end stations. DIFS is the longest of the fixed interframe spaces. When starting a contention period, stations are required to wait until the DIFS has expired before contending for network access.

Copyright © 2003, Planet3 Wireless, Inc.


Collision Handling
• CSMA/CA vs. CSMA/CD
• Wireless LANs use collision avoidance and acknowledgements
8-5 CWNA-MAC & Physical Layers
Copyright 2002 Planet3 Wireless, Inc.
cwna

client client can't get the ack from other client.

hidden node: client can't see each other clients can see AP.

RTS: all clients can see AP. AP can see RTS packets to the client to ask client to send packets.

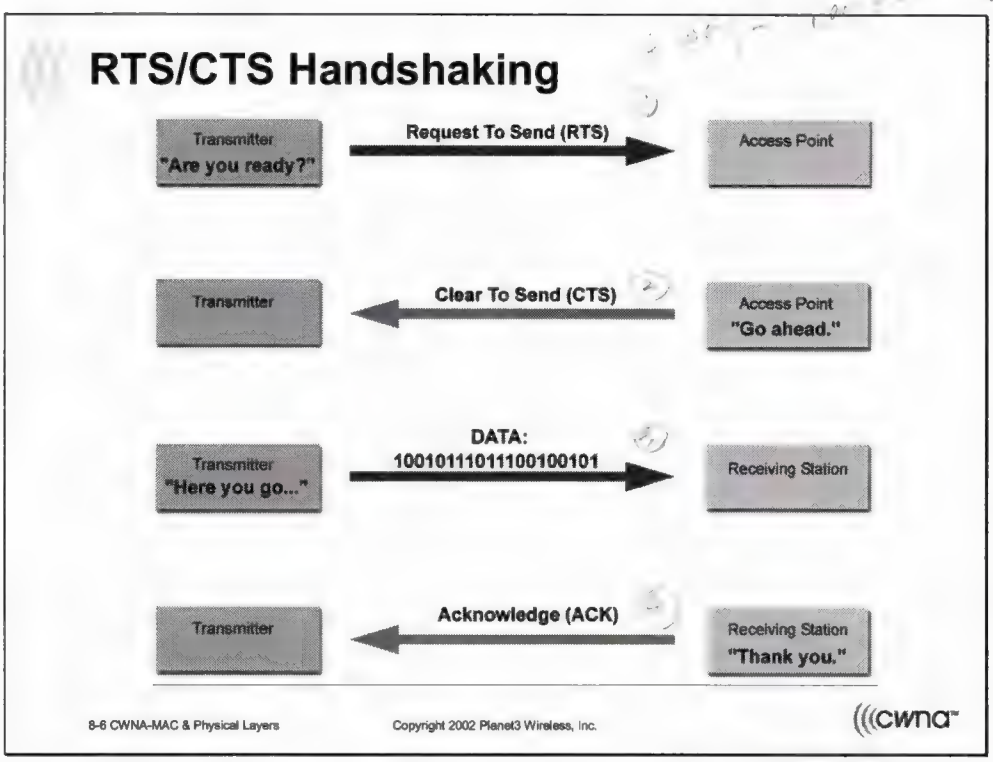
CSMA/CA is a contention-based protocol

Collision Handling

The biggest difference between CSMA/CA (used for wireless LANs) and CSMA/CD (used for Ethernet) is that CSMA/CA avoids collisions and uses positive acknowledgements (ACKs) instead of arbitrating use of the medium when collisions occur.

It is impossible to detect a collision in a wireless LAN so a mechanism has to be in place to handle a collision situation. This mechanism is accomplished through ACKs. When a station transfers a frame to another station, the receiving station immediately replies with an ACK so that the transmitting station knows that there was not a collision. If no ACK is received back, the transmitting station assumes a collision happened and resends the frame.

Use of CSMA/CA imposes approximately 50% overhead so that throughput of the network is approximately 50% of rated bandwidth. By comparison, CSMA/CD has approximately a 30% overhead with very low user counts. On a saturated network or with heavy use, CSMA/CD can cause overhead of approximately 70%.



Request-to-Send / Clear-to-Send

Request-to-Send / Clear-to-Send (RTS/CTS) is a protocol used to allow stations to announce their intention to transmit data across the wireless network. RTS/CTS is an extension to CSMA/CA and is used for the purpose of cutting down on collisions due to wireless LAN-specific problems such as the hidden node problem (discussed in Troubleshooting).

RTS/CTS uses a four-way handshaking process, as illustrated above. First, the transmitting station broadcasts the RTS, followed by the CTS reply from the receiving station. Next, the transmitting station sends its data payload through the access point to the receiving station that immediately replies with an acknowledgement frame, or ACK. This process is used for every frame transmitted across the wireless network when RTS/CTS is enabled and the threshold is exceeded.

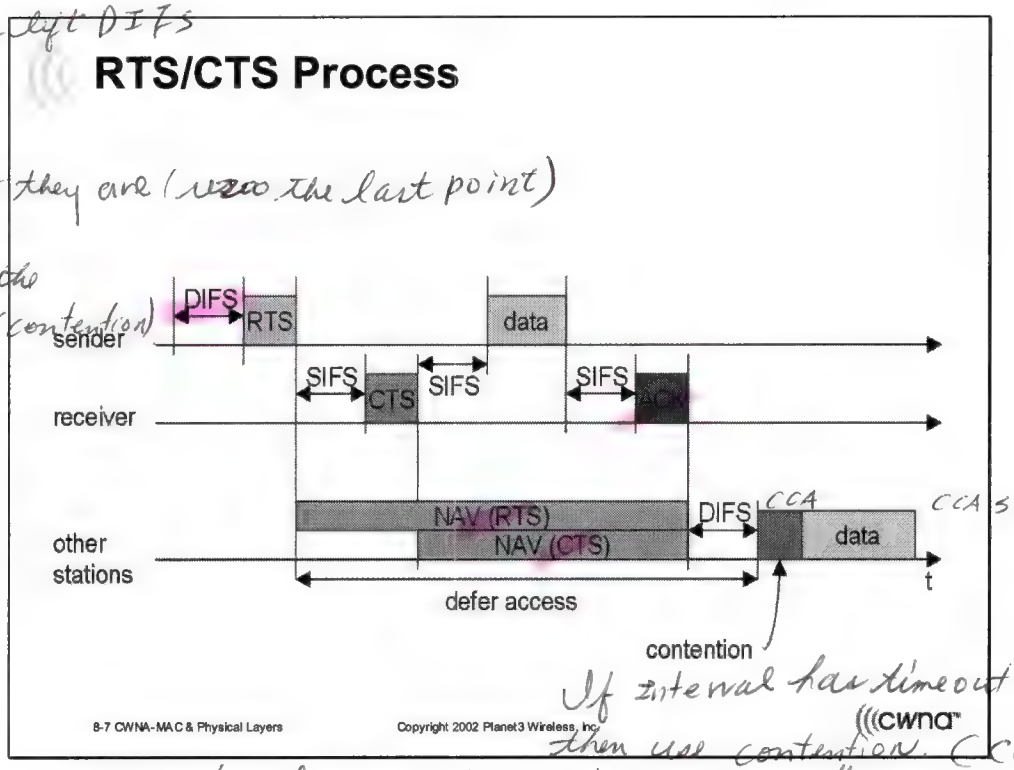
Note RTS/CTS adds a great deal of overhead and should not be used unless the throughput is already poor due to collisions. Normally this feature would be turned off.

Copyright © 2003, Planet3 Wireless, Inc.

Network allocation victors:
- ~~DIFS~~ RTS/CTS
- ACK
- your own time left DIFS

time / don't reset
get back what they are (not the last point)

all clients back to the same "~~time~~ beginning" (contention)



CCA SIFS ACK

If interval has timeout then use contention (CCA)

Clear channel assesment (CCA)

Do I hear any signal greater than threshold
Yes - wait
No

RTS/CTS Process

1. A wireless node broadcasts its intention to send a message to another station or to the access point by sending a "Request-to-Send" (RTS) message. All stations within reception range of the transmitting station set their Network Allocation Vector (NAV) field to the number of time slots needed for the station to transmit the necessary data and to receive the ACK.

   The NAV field in each station acts like a timer. It counts down from a value set by the RTS and/or CTS frames. When a station's NAV field equals zero, it can begin contending for network access again.

2. The receiving station responds to the RTS with a "Clear-to-Send (CTS)" message that causes all stations within range to reset their NAV field (again) to the amount of time necessary for the transmitting station to transmit its data and to receive the ACK.

3. Upon receiving the CTS message, the initiating station begins transmission of its DATA.

4. The receiving client immediately sends an ACK frame to acknowledge receipt of the DATA and network contention begins again. Completion of the ACK should coincide with the time all other stations finish counting down their NAV field to zero.

RTS/CTS Configuration

RTS/CTS is configured on the client and the access point. There are three settings for RTS/CTS:

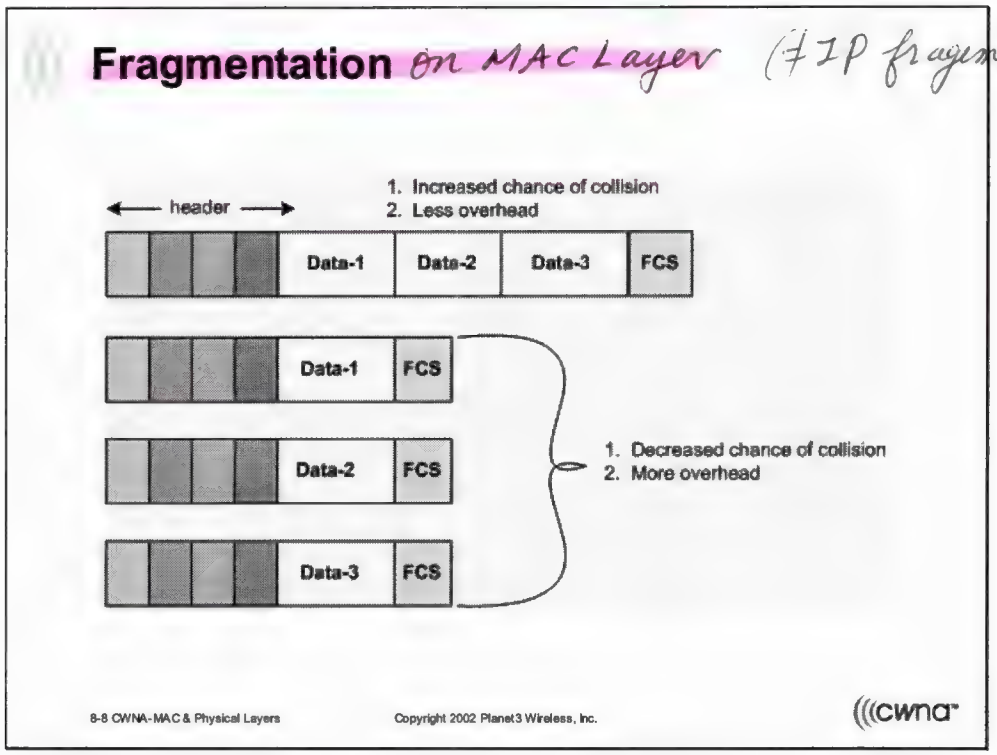
- Off
- On
- On with threshold

The "On with threshold" setting is used so that administrators can fine-tune network performance. It is important to understand the effects of changing the RTS/CTS threshold before making any changes. The threshold value is a packet size specified by the administrator. Changing the packet size threshold has the following effects:

Making the packet threshold smaller - setting the packet threshold to trigger use of RTS/CTS with smaller packets can cause many more packets to use the RTS/CTS protocol, which will add significant overhead to the network.

Making the packet threshold larger - setting the packet threshold to trigger use of RTS/CTS with larger packets means that only packets larger than the threshold size will use the RTS/CTS protocol, which should optimize throughput. Larger packets are more likely to experience collisions on a wireless network because they take longer to send. Using RTS/CTS only with larger packet sizes is a practical way to achieve optimum throughput in a busy wireless LAN environment. An important note is that RTS/CTS is mandatory as specified by 802.11 for frames larger than 2347 bytes.

Copyright © 2003, Planet3 Wireless, Inc.



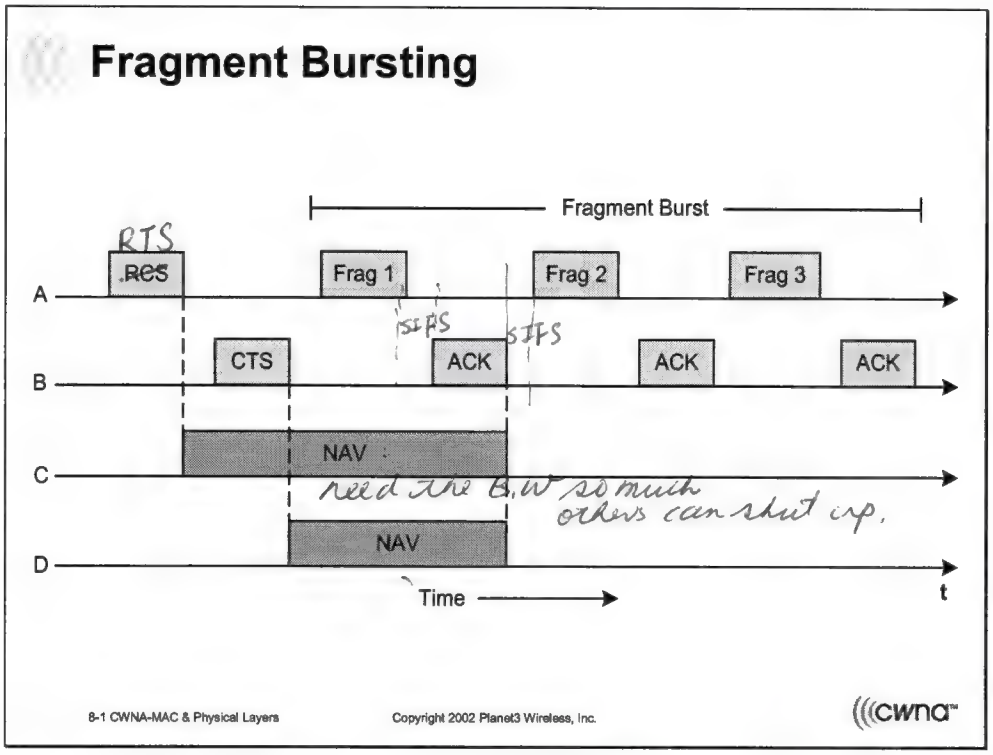
Fragmentation

Fragmentation of packets into shorter fragments adds protocol overhead and reduces protocol efficiency (decreases network throughput) when no errors are observed, but reduces the time spent on re-transmissions if errors occur. Larger packets have a higher probability of collisions on the network; hence, a method of varying packet fragment size is needed. The IEEE 802.11 standard provides support for fragmentation.

By decreasing the length of each packet, the probability of interference during packet transmission can be reduced. There is a tradeoff that must be made between the lower packet error rate that can be achieved by using shorter packets, and the increased overhead of more frames on the network due to fragmentation. Each fragment requires its own headers and ACK, so the adjustment of the fragmentation level is also an adjustment of the amount of overhead associated with each packet transmitted. Stations never fragment multicast and broadcast frames, but rather only unicast frames in order not to introduce unnecessary overhead into the network. Finding the optimal fragmentation setting to maximize the network throughput on an 802.11 network is an important part of administering a wireless LAN. Remember that a 2346 byte frame is the largest frame that can traverse a wireless LAN segment without fragmentation. Keep in mind that the layer 3 protocol in use will generally determine that packets no larger than 1500 bytes are used across the wired and wireless LANs.

Copyright © 2003, Planet3 Wireless, Inc.

RTS/CTS
NAV
SIFS
wait for another SIFS
send packet 2
DIFS



Fragment Bursting

As we previously discussed, the IEEE 802.11 standard allows frames to be fragmented into smaller pieces. Each fragment is uniquely numbered and is acknowledged by the recipient. In this way, the sending station cannot transmit the next fragment until the previous fragmented has been acknowledged. However, once the channel has been acquired via the RTS and CTS mechanism, multiple fragments can be sent in a row; this is called a fragment burst.

Typically, the NAV mechanism only keeps other stations from transmitting until the next ACK is sent. Fragment bursting allows an entire fragment burst to be sent without interference or interruption. Just as SIFS is used to allow stations to send an RTS, send a CTS or send an ACK, it can also be taken advantage of to send the next fragment in a group without the sending station needing to send another RTS again.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

9 Troubleshooting Wireless LAN Installations

Objectives

Upon completion of this chapter you will be able to:

- Define multipath and its effects on RF transmission
- Understand how antenna diversity helps solve the problem of multipath
- Identify and resolve the issues with hidden nodes and Near/Far
- Understand how to maximize the throughput of DSSS systems using co-location
- Identify common types of interference and how to work around them

9-2 CWNA-Troubleshooting Wireless LAN Installations

Copyright 2002 Planet3 Wireless, Inc.

Chapter Content

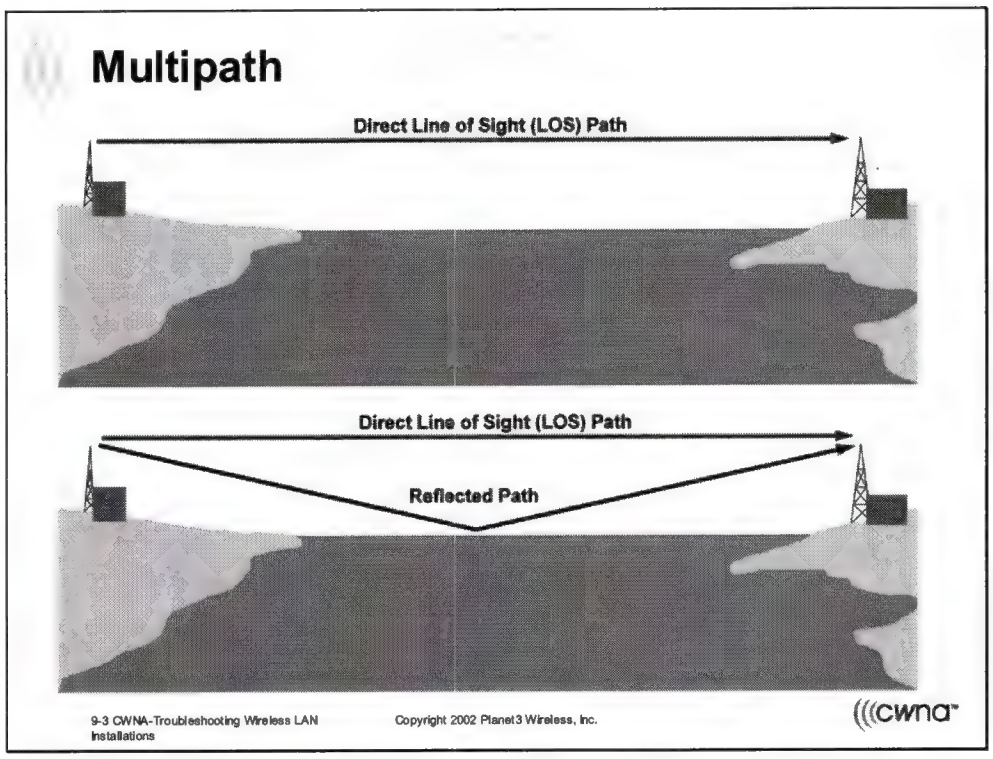
Wireless LAN installations have a number of issues that may come up during configuration and administration that are not found in typical wired networks. Because the transmission medium of the data is RF instead of copper wire, administrators need to be aware of how these signals can be affected in various situations. A wireless LAN connection can be disrupted or interfered with by a number of things. These problems can cause loss of connection, corrupted data, and other symptoms, even when the connection has been functioning correctly for a period of time.

This chapter covers the most common wireless LAN connectivity problems and their solutions.

The chapter outline follows:

- Multipath
- Antenna Diversity
- Hidden Nodes
- Near/Far
- Co-location Throughput
- Interference

Copyright © 2003, Planet3 Wireless, Inc.



Multipath

Multipath is the composition of a direct signal plus reflected signals that have bounced off objects between the transmitter and receiver. Multipath can reduce or completely cancel throughput in a wireless LAN. Direct and reflected RF wave fronts are additive at the receiver.

Ideally, an RF transmission will take only the direct LOS path; however, RF waves will likely be reflected off nearby objects creating multiple wave fronts. The strongest received wave front is that of the direct path between transmitter and receiver, but because a wave front grows wider as it propagates, it will hit objects around the direct path such as bodies of water, metal roofs, etc. The signal reflects off these objects resulting in multiple wave fronts arriving at the receiver.

There are 4 resultant problems that multipath can cause to the wave front at the receiving end of the link:

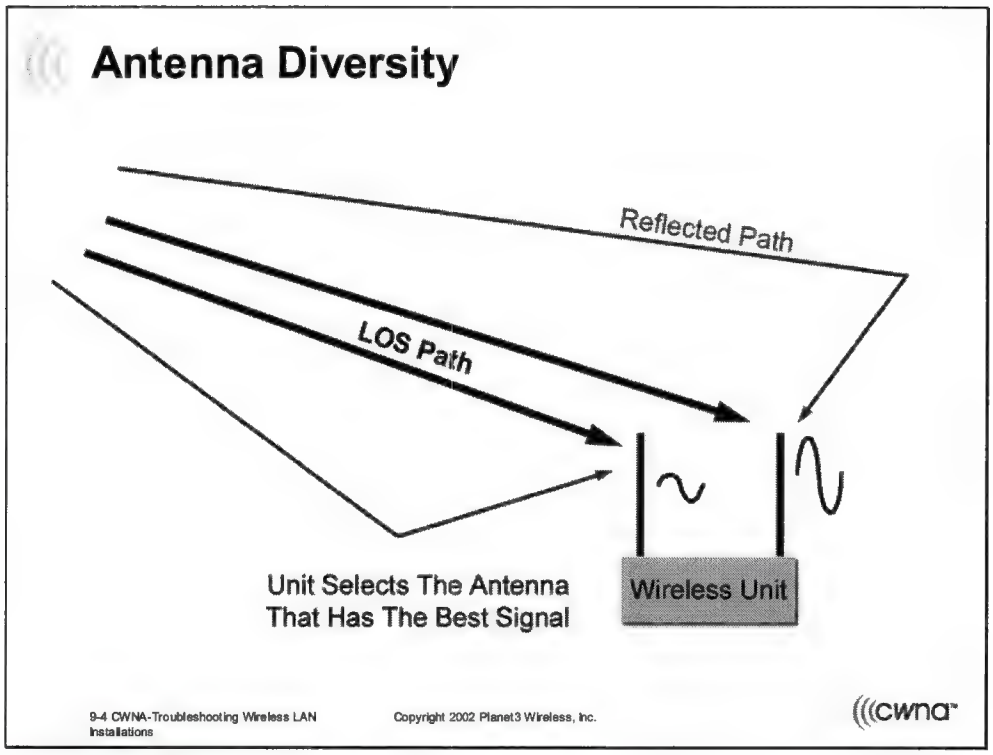
1. Corrupted Data - caused by the receiver getting a strong enough signal coming from the reflected path to effectively render the main signal unreadable. This condition generally occurs when the reflected signal itself is distorted or unreadable.
2. Signal loss (nulling) – the main signal and the reflected signal cancel each other out resulting in no signal being received. This condition occurs when the reflected signal is reflected out of phase with the main signal, but is still strong enough to significantly affect the receiver's ability to discern the main signal.

3. Signal degradation (downfade) – degradation (reduced amplitude), of the main signal due to reflected signals being out of phase with the main signal, but not of enough amplitude to cancel (or null) the main signal
4. Signal increase (upfade) – an increase in the received signal (increased amplitude) due to the reflected signal being in phase with the main signal at the receiver.

Note The signal at the receiver will never be larger than the signal at the transmitter. The received signal can be increased over what it would have been if there had been no multipath, but it cannot be larger than the source signal. Recall that the signal will always significantly decrease due to free space path loss. Free space path loss assures that the received signal will always be smaller than the transmitted signal.

Delay spread is the time between the first signal received and the last reflected signal received and can be up to 4 ns in duration.

Copyright © 2003, Planet3 Wireless, Inc.



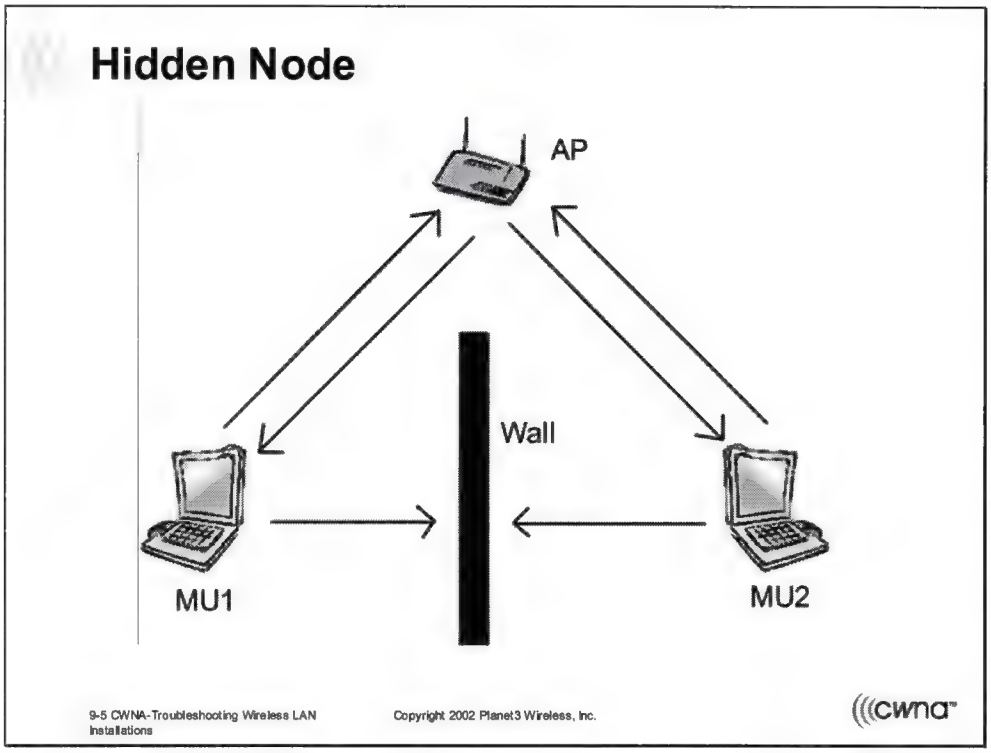
Solution of multipath

Antenna Diversity

Antenna diversity is the use of multiple antennas in order to compensate for the negative effects of multipath. Antenna diversity works by having multiple antennas on multiple inputs into one receiver. The receiver samples each input constantly, comparing the received signals of each to determine which is best.

Signal Reception and Transmission

The signal is received into the receiver through one antenna at a time, and the receiver transmits out through the antenna last used for reception. The last antenna from which a signal is received is used to send a transmission because it is assumed that this antenna would have the better connection. An access point is a half-duplex environment, so the device can send or receive, but not both at the same time. The radio can alternate retransmissions between antennas.



Hidden Node

Hidden node occurs when two wireless clients cannot hear each other's transmissions, but the access point can hear both clients. One client may start transmitting not realizing that another client is currently transmitting, causing excessive collisions on the network. Poor throughput on a wireless network may be a sign of a hidden node.

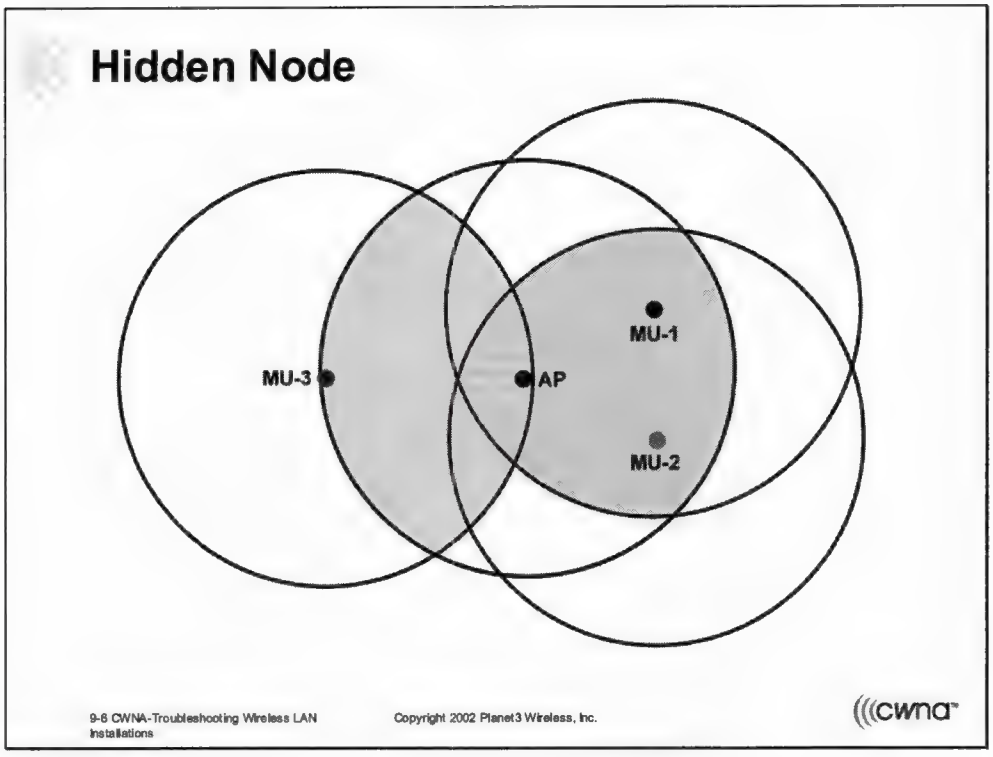
In the illustration, all mobile units can communicate with the access point; however, MU-1 and MU-2 are hidden from MU-3. If MU-3 starts transmitting to the access point at the same time MU-1 or MU-2 are transmitting, collisions will occur.

Solutions for Hidden Nodes

Use of RTS/CTS

To isolate the problem, RTS/CTS can be turned on to see if network performance improves. Use of RTS/CTS adds network overhead, but it can be used in this case to isolate a network bottleneck. If RTS/CTS is turned on and the throughput increases, it indicates that there were substantial collisions on the network likely due to a hidden node.

Copyright © 2003, Planet3 Wireless, Inc.



Use of RTS/CTS (continued)

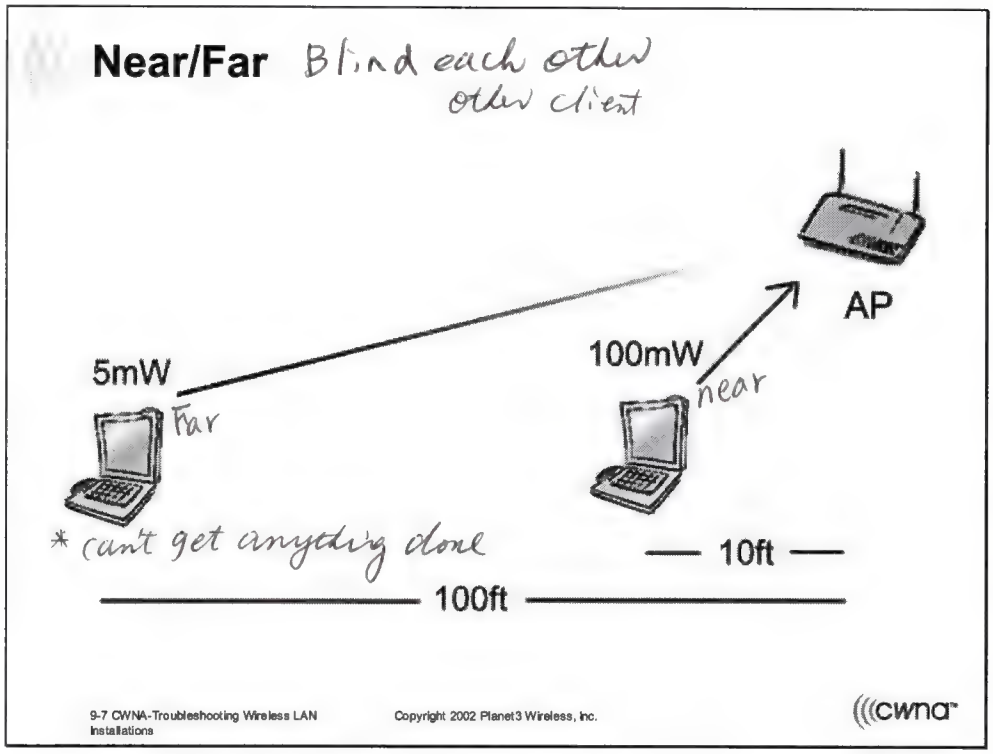
An access point has three settings for RTS/CTS – off, on, and on with threshold (packet size). For thresholds, the access point can be configured to use RTS/CTS for every packet that exceeds a certain size. The RTS/CTS overhead can be avoided in all but the special cases of large packet sizes using this method. Larger packets are more susceptible to collisions because they take more time to transmit, which is where the network would benefit from use of RTS/CTS.

Increasing Power to Nodes

Increasing the power output of the stations would increase their transmission radius, allowing other stations to hear their transmissions.

Removing Obstacles

Any obstacles that are between stations that may be causing the problem should be addressed, such as filing cabinets or metal obstructions. If the obstacle turns out to be a physical wall that is causing the problem, the design of the wireless LAN will need to be addressed to see how the problem can be solved.



Near/Far

Near/Far is caused when network stations in close proximity (near) transmitting at high-power blind each other to more distant (far) stations whose power output is much smaller. The far station is effectively cut off from the network.

As can be illustrated by the above image, the station outputting 100mW is overpowering the station farther away transmitting at 5mW.

Solutions for Near/Far

Near/Far is an indication of network design problems that need some type of correction to improve communication. Possible solutions might include:

Increase Far Node's Power

Increasing the power on the far station will increase its coverage range, allowing near stations to see the far station's traffic. When near stations can hear far stations, the Near/Far problem is eliminated because near stations will allow the far station to participate as part of the network.

Copyright © 2003, Planet3 Wireless, Inc.

- **Decrease Near Node's Power**

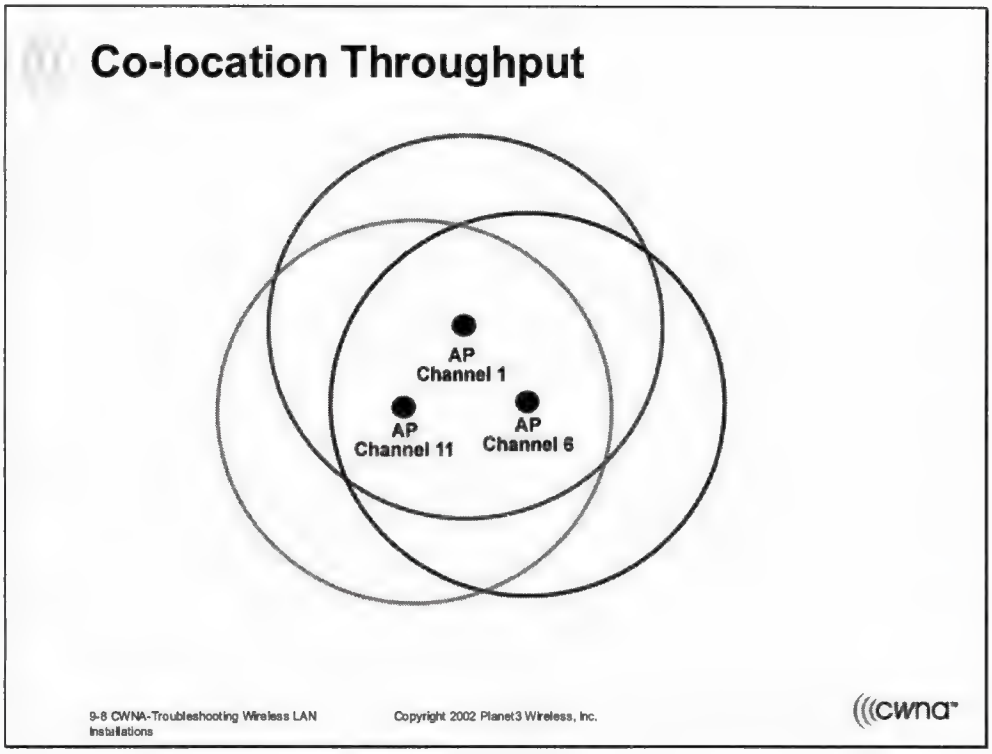
  This solution is the reverse of increasing the far station's power. Reducing the near station's output power will have the same result as increasing the far station's output power. Near stations should now be able to hear the transmissions of the far station.

- **Move Remote Node**

  Moving the far station closer to the near stations effectively increases the far station's signal. Just as the perceived volume of a sound gets louder the closer it is to the receiver, so does the RF output signal deliver more energy into the receiver by being closer to it. By moving the far station closer to the near stations, the path loss of the far station is reduced.

Role of Access Protocol

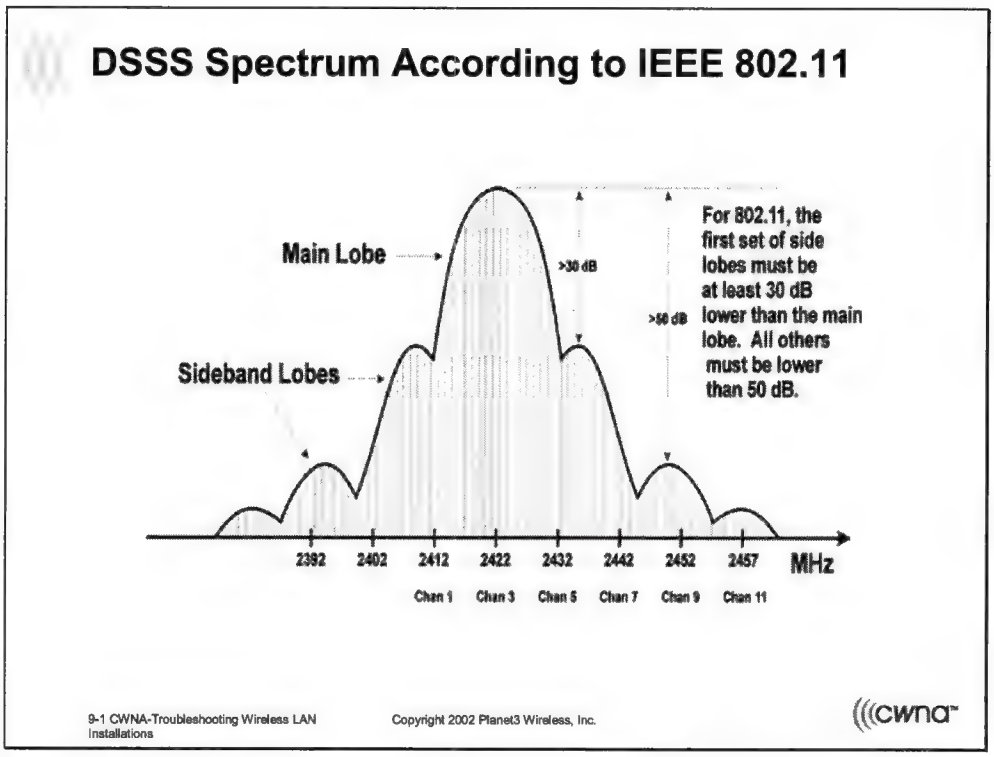
The CSMA/CA protocol is designed to alleviate a large portion of the Near/Far problem. According to the CSMA/CA rules, any station hearing another station transmitting shall not transmit, so if the near station(s) hear the far station(s), then they know to cease transmission. The problem is that sometimes these near stations cannot hear the far station, and thus, the CSMA/CA protocol does not help.



Co-location Throughput

Co-location is a method of installing multiple access points using different channels in the same location to increase overall throughput in a wireless LAN.

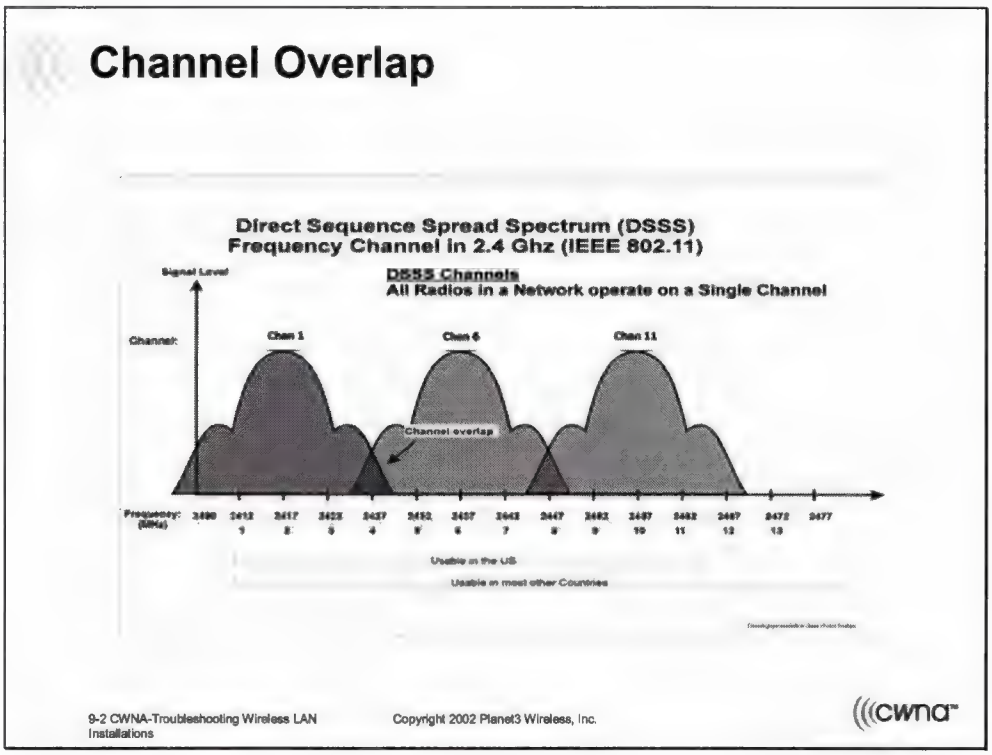
Copyright © 2003, Planet3 Wireless, Inc.



Theory vs. Real-World

In theory, when using DSSS, three non-overlapping channels (1, 6, and 11) can be used, and maximum throughput will be achieved on each channel. In real-world scenarios, the theory does not hold true. There is 3 MHz of separation between these three non-overlapping channels. Theoretically, 3 MHz should be plenty of channel separation in order to avoid adjacent channel interference, but that is not true for all situations. Depending on the distance between access points, the manufacturer's hardware used, and background RF noise in the environment, and the output power of each transmitting node, much throughput can be lost due to "non-overlapping" channels experiencing adjacent channel interference.

Adjacent channel interference is caused when channels that are side-by-side overlap each other causing signal degradation to both channels. Sometimes, one channel is affected more than the other by this type of interference.



DSSS Co-location Best Practice

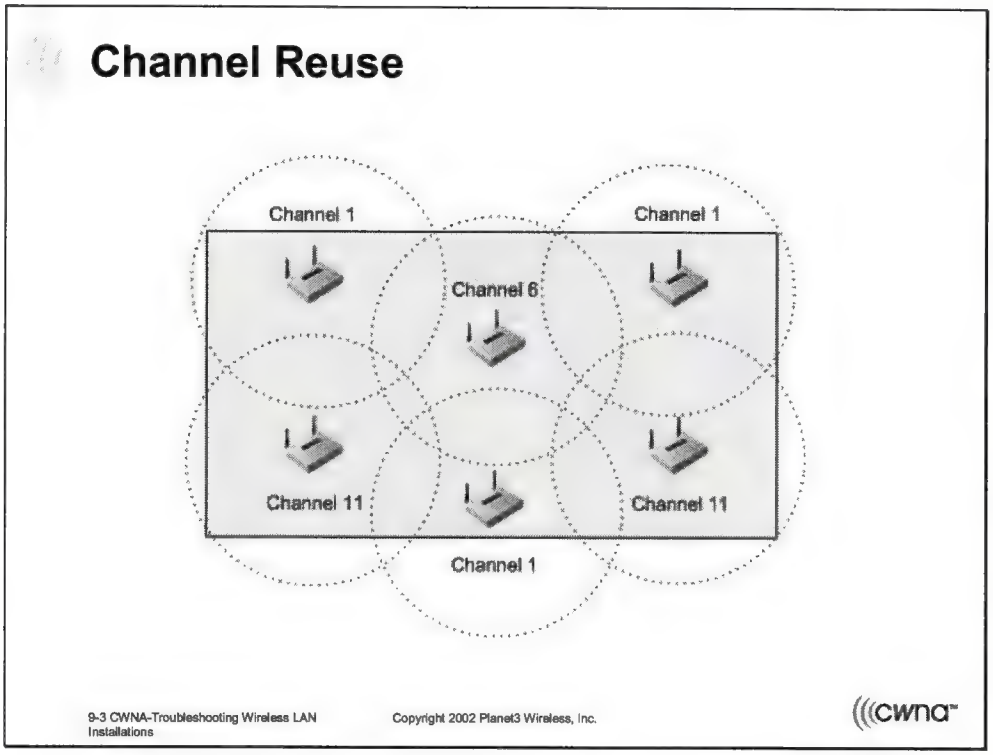
DSSS has three non-overlapping channels that actually do interfere with each other (under given circumstances) in a co-located environment, resulting in reduced throughput on each of the three channels. The middle channel slightly overlapping the other channels can cause DSSS interference over the 3 channels. Take the case where channels 1 and 11 are used. The maximum throughput for these channels may be ~5 Mbps. When all 3 channels are used, the throughput for each channel may drop to as low as 4 Mbps due to adjacent channel interference.

The best configuration for co-location of DSSS systems is on channel 1 & 11 or another pair of similarly spaced channels. For example, channels 2 & 10 or 3 & 9 would do nicely due to a large amount of frequency separation. If use of channels 1, 6, & 11 is necessary, the access points should be spaced far enough apart to where there is minimal interference between them. By adequately spacing access points while having them configured for channels 1, 6, & 11, a situation is created where the signal amplitude of each unit is so low (due to path loss and absorption by nearby objects) that by the time it reaches the other units, the adjacent channel interference is eliminated. This spacing scenario is the most common in real-world application.

Another point of consideration when placing access points deals with configuring them for failover/hot-standby and load-balancing. Many enterprise quality access points, such as those from Cisco, now include some form of software support for hot-standby and load-balancing. Additionally, some access points (such as those from Orinoco) contain two separate radios that can be used for load-balancing

Copyright © 2003, Planet3 Wireless, Inc.

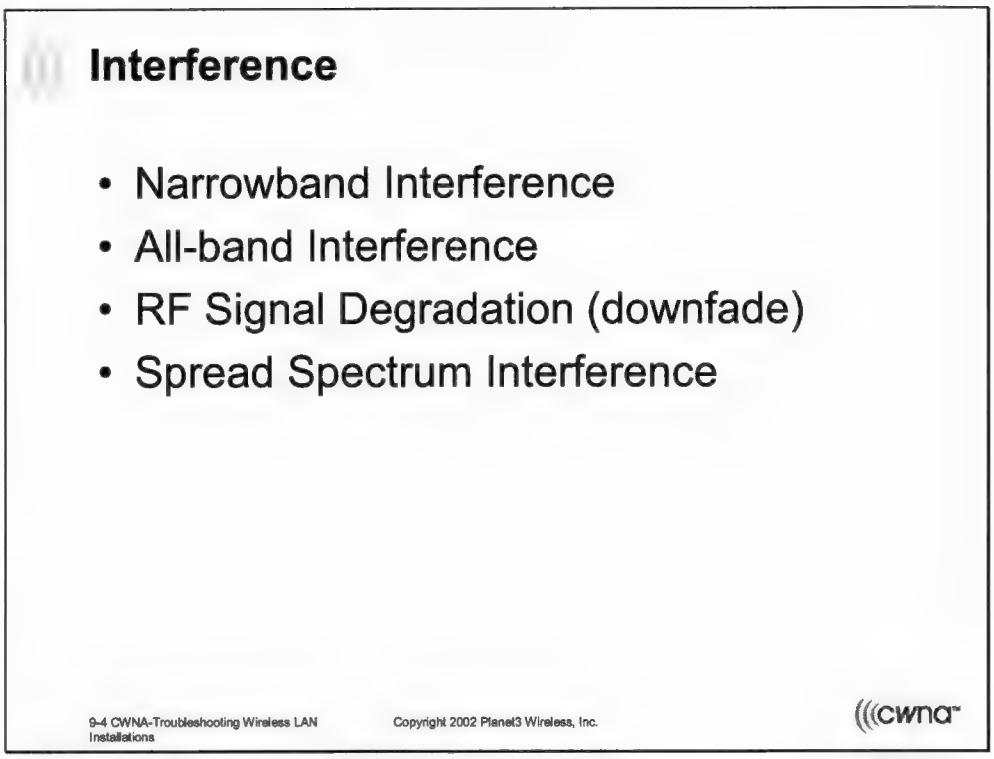
within a single access point. These points should be part of your planning and design if required.



Channel Reuse

In situations where seamless roaming is required, a technique called channel reuse is used in order to alleviate adjacent and co-channel interference while allowing users to roam through adjacent cells. Channel reuse is the side-by-side locating of non-overlapping cells to form a mesh of coverage where no cell on a given channel touches another cell on that channel.

Copyright © 2003, Planet3 Wireless, Inc.



Interference

Interference of an RF signal is anything that can hinder, obstruct, or impede the signal from being received in a usable form.

Narrowband Interference

Narrowband interference is generally caused by a stationary, high-power RF broadcast on a narrow band of frequencies from a non-wireless LAN source. Some sources of narrowband RF interference might include:

- Microwave ovens
- Elevator motors
- RF signal generators

Spread spectrum RF systems are designed to overcome a certain amount of narrowband interference by virtue of spreading the transmitted information over a broad band of frequencies.

All-band Interference

All-band interference refers to interference that spans the entire useable band of frequencies (regardless of frequencies used). All-band interference causes wireless LANs to be unable to operate depending how severe the interference is. Sources of all-band interference might include:

- Plasma cutters
- RF Sweep or Comb generators
- Bluetooth

Spread Spectrum Interference

RF Interference can be caused by spread spectrum systems as well. Some sources of spread spectrum interference might include:

- Other nearby wireless LANs or their reflections
- Baby Monitors
- Spread spectrum phones
- Industrial, Scientific, or Medical equipment

Adjacent and Co-channel Interference

Adjacent channels are channels that are side-by-side in the frequency spectrum. The overlapping of these channels can cause interference for each channel. For example, if channel 1 overlaps channel 4, adjacent channel interference can occur.

Co-channel interference occurs when an access point on a given channel interferes with a nearby access point on the channel.

Physical Interference

Downfade is a term used by some manufacturers to describe degradations in the RF wavefront's amplitude. Downfade (a reduction in signal amplitude) may be caused by multipath, poor RF line of sight, blockage of the Fresnel Zone, severely adverse weather conditions, co-channel interference, and adjacent channel interference.

Poor RF Line of Sight

Poor RF LOS can occur due to obstructions in the direct path of the RF wave front that exceed 20-40% blockage of the Fresnel Zone.

Copyright © 2003, Planet3 Wireless, Inc.

Severely Adverse Weather Conditions

Rain, fog, snow, and hail *do not* have a significant impact on wireless LAN performance. Conditions that do significantly affect the signal are lightning, wind, and air stratification. Lightning can destroy a wireless LAN and wind can cause antenna loading.

Antenna loading is a situation in which the wind blows against the antenna to the point of moving it from its stationary position. This occurrence can cause disruption in service due to a broken wireless link.

Air stratification occurs when the air gets very still and is separated into layers. When RF wave fronts pass through stratified air, it causes bending of the wave front and some amount of reflection. Smog, due to chemicals and layering of the air, can cause problems for wireless LANs.

Rain, fog, snow, and hail may have some minor effects depending on how severe they are, but for the most part, these weather conditions do not cause significant problems for a wireless LAN.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

10 Wireless LAN Security

Objectives

Upon completion of this chapter you will be able to:

- Define and describe WEP and its features
- Define and describe AES and other emerging security solutions
- Detect the different methods of attacking a wireless network
- Discuss wireless security management
- Contrast security solutions

Copyright 2002 Planet3 Wireless, Inc.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter Content

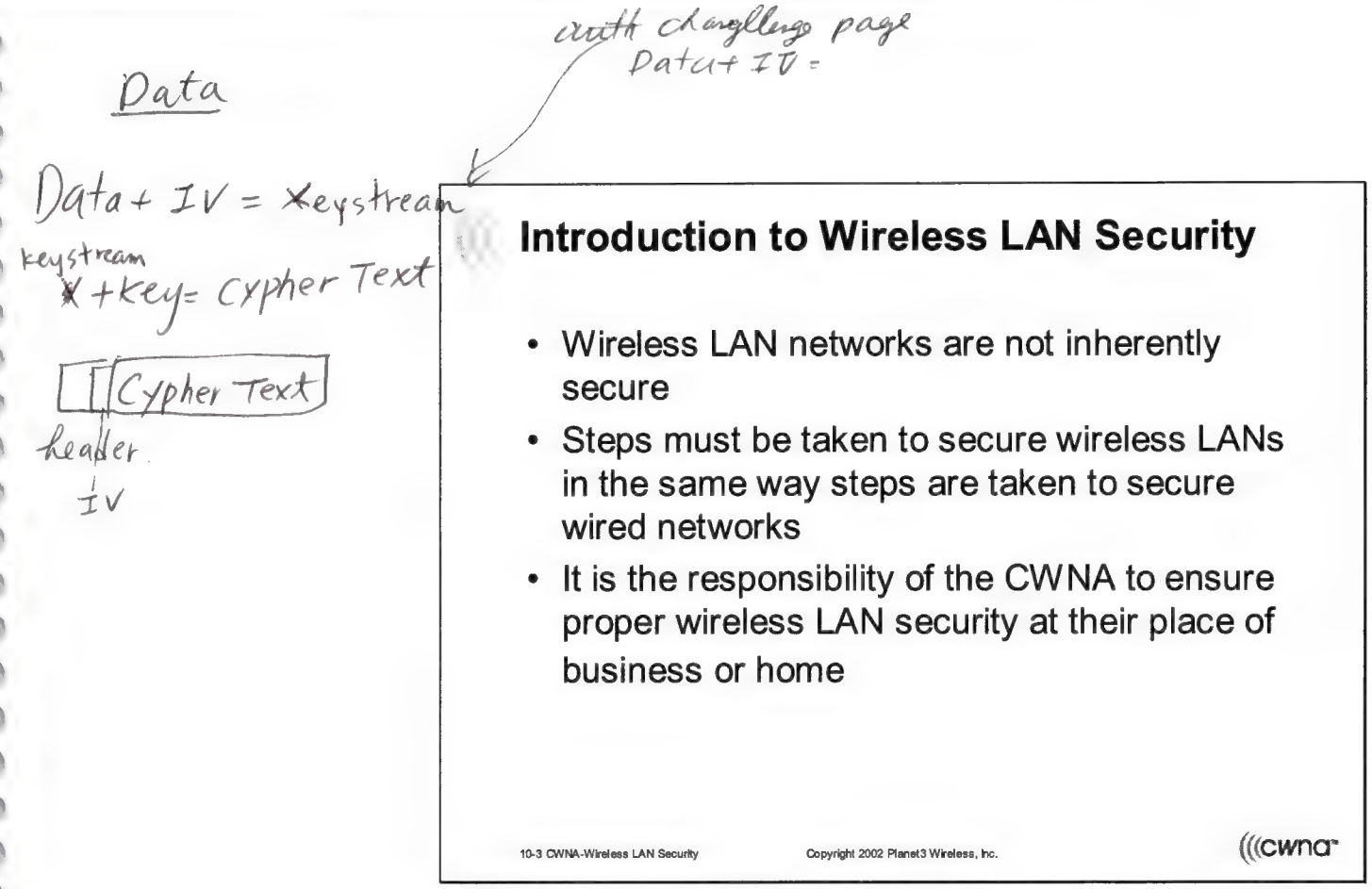
Wireless LAN security is a frequent topic in technology news. The subject most discussed is how easy it can be for a hacker to gain access to a wireless LAN and compromise the data that lies on the wired network. Wireless LAN security is therefore a high priority for any organization that has an existing wireless LAN or is considering implementing a wireless LAN. The task of making or keeping data secure rests with the wireless LAN administrator.

This chapter covers IEEE 802.11's Wired Equivalent Privacy (WEP), why it is not secure, and what will be replacing it. The different types of wireless LAN attacks are shown, and managing wireless LAN security is discussed. This chapter ends with discussions on implementing corporate wireless security policy and recommendations for securing a wireless network.

The chapter outline follows:

- Introduction to Wireless LAN Security
- Wired Equivalent Privacy
- How Attacks Occur
- Managing Wireless Security
- Corporate Security Policy
- Security Recommendations

Copyright © 2003, Planet3 Wireless, Inc.

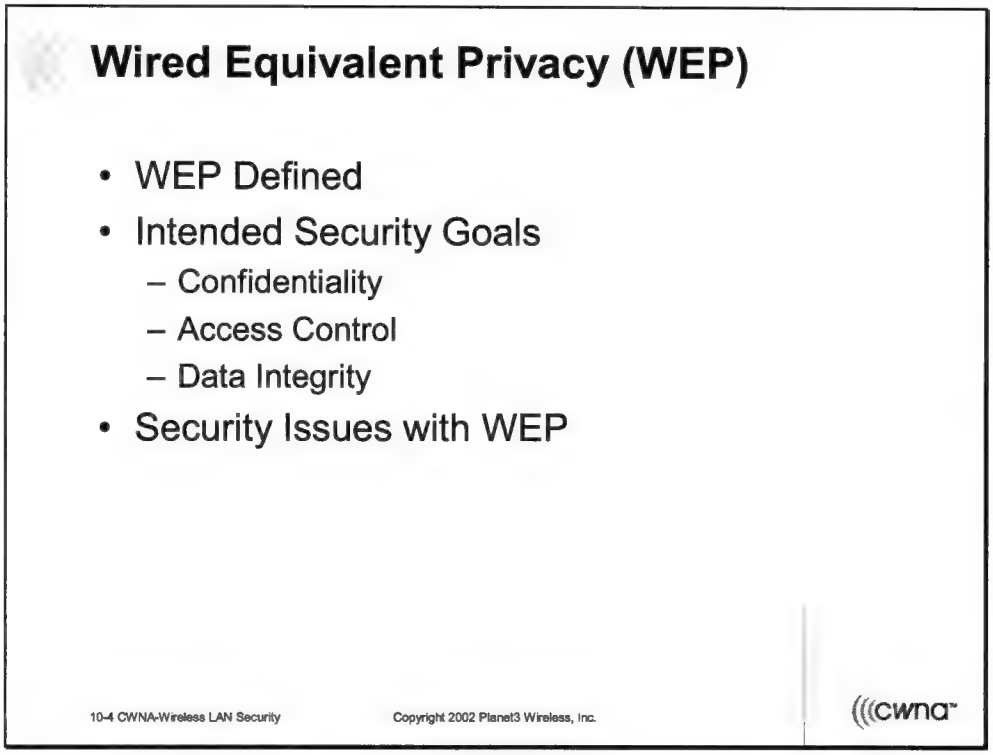

auth challenge page
Data + IV =
Data
Data + IV = Keystream
keystream
X + key = Cypher Text
Cypher Text
header
IV
Introduction to Wireless LAN Security
• Wireless LAN networks are not inherently secure
• Steps must be taken to secure wireless LANs in the same way steps are taken to secure wired networks
• It is the responsibility of the CWNA to ensure proper wireless LAN security at their place of business or home
10-3 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

Introduction to Wireless LAN Security

Wireless LANs are not inherently secure. Steps must be taken to secure wireless LANs in the same way steps are taken to secure wired networks.

The standard method of authentication on a wired network is a username and password. This same type of functionality is needed on a wireless network. Vendors are now introducing solutions that add username and password authentication processes.

It is the responsibility of the CWNA to ensure proper wireless LAN security at their place of business or home. The administrator's job is to make sure the network meets whatever security levels deemed to be necessary by the IT Director.



Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an encryption algorithm used for encrypting data payloads over the wireless segment of the LAN using keys. WEP is not used end-to-end, but rather across the wireless portion of the network only (from the client to the access point). WEP keys can also be used for Shared Key authentication.

Security Goals

WEP was intended to support the following security goals:

- Confidentiality – encryption of the data so unauthorized viewers cannot read the data.
- Access Control – controlled access onto the network by accepting or denying connections.
- Data Integrity – provides a means of checking the data to make sure what was sent is the same as what was received. This is important for when hackers attempt to modify data in-transit from source to destination.

Copyright © 2003, Planet3 Wireless, Inc.

Security Issues

WEP is not secure, and has one major weakness. WEP is a simple (weak) algorithm that uses the RC4 stream cipher. What makes WEP weak is how it implements the RC4 stream cipher and its 24-bit Initialization Vector (IV). Both 64-bit and 128-bit WEP use the same encryption process.

The IV is transmitted in the clear, causing:

- *Active attacks to inject new traffic*- Unauthorized mobile stations can inject packets onto the network based on known plaintext
    1. Knowledge of one packet could be used to create other, seemingly legitimate packets.
    2. Theoretically this is possible even if there is only partial knowledge of the contents of an encrypted packet.
    3. Can be used to interact with servers on the wired network (open shells, modify files, etc.).
- *Active attacks to decrypt traffic* - Can be used to "trick" the AP into revealing the plaintext of any traffic on the network.
    1. Involves capturing encrypted traffic and modifying the header information.
    2. The modified traffic is sent to some server on the Internet controlled by the attacker.
    3. The AP will decrypt any traffic before placing it on the wired network.
    4. This traffic shows up at the server in its plaintext form.
- *Dictionary-building attacks* - After gathering enough traffic, the WEP key can be cracked using freeware tools. Once the WEP key is cracked, real-time decryption of packets can be accomplished by listening to broadcasts packets using the WEP key. This type of attack can be accomplished due to the limited space in the 24-bit IV.
    1. Once the plaintext for a packet has been revealed, the RC4 stream can be computed on a "per IV" basis.
    2. Given enough time and storage space an IV table could be built.
    3. Once the table is built, traffic can be decrypted in near real time.
    4. The Berkeley paper estimates that roughly 15GB of traffic would need to be gathered for a complete table.
- *Passive attacks to decrypt traffic* - Using statistical analysis, WEP traffic can be decrypted as follows:
    1. By performing cryptographic analysis on IV collisions, the original plaintext can be determined.
    2. Much of the traffic is predictable (AP beacons, ARP requests) and also includes much redundancy.
    3. This redundancy can be used to eliminate certain content and increase accuracy.
    4. When the plaintext for one packet is recovered, the plaintext for all similar IVs will soon follow.
    5. This can be aided by sending traffic from the internet to a specific wireless host.

Copyright © 2003, Planet3 Wireless, Inc.

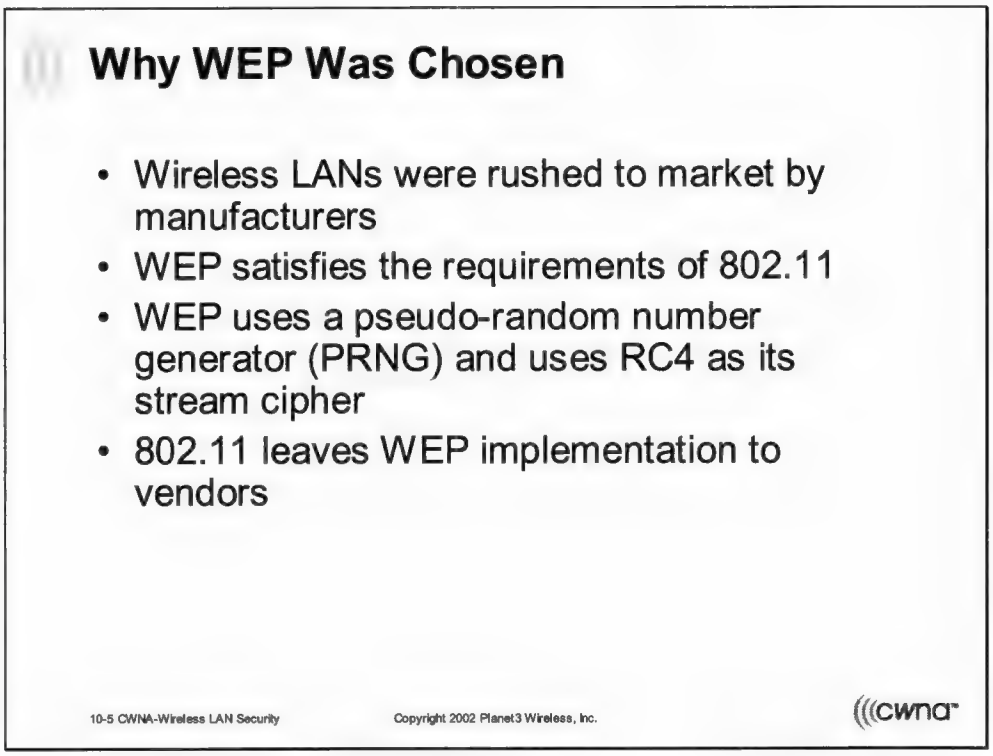
Most implementations of WEP initialize hardware using an IV of 0, and thereafter incrementing the IV by 1 for each packet sent. Because the IV is broadcast in the clear, it can easily be read with a packet analyzer. An analyzer would show the IV incrementing, and the hacker can jump in where the last IV left off.

WEP can be cracked in a relatively short period of time using off-the-shelf hardware and easily obtained freeware hacking utilities such as Airsnort and WEPcrack. Statistical modeling has been done that shows that all available IVs (2^{24}) would be used in a busy network in a 5 hour period time (perhaps even less)—meaning that the IV would be reinitialized starting at zero once every five hours. The repeating of the IV makes it just that much easier for a WEP cracking application, such as Airsnort, to gather enough network traffic in order to be able to reverse engineer the WEP key. Airsnort, for example, boasts that it only needs between 100 MB to 1 GB of data in order to successfully crack WEP. The means by which these applications are able to crack WEP are actually fairly simple to understand. If you collect many pieces of data that all have one thing in common, you will eventually be able to determine that one thing despite any amount of encryption in place. This one thing in common is, of course, the static WEP key. The RC4 algorithm is public domain, thus it can be reverse engineered. The strength of WEP lies in keeping the WEP from being discovered by an intruder. Once the key has been comprised, an intruder can "sniff" the network in clear text and gain access to resources past the access point.

TKIP, now approved by the Wi-Fi Alliance for inclusion in all Wi-Fi certified products, should start to become a very big reality in the early part of 2003. TKIP (Temporal Key Initialization Protocol) corrects the inherent weaknesses that have been identified in WEP. Although IEEE 802.11i is still over a year away from being a reality, TKIP is a substantial security improvement that is already available.

Note It should be noted that the RC4 stream cipher can handle keys as large as 256 bits. WEP, however, only uses the two smaller sizes discussed previously.

Copyright © 2003, Planet3 Wireless, Inc.


Why WEP Was Chosen
• Wireless LANs were rushed to market by manufacturers
• WEP satisfies the requirements of 802.11
• WEP uses a pseudo-random number generator (PRNG) and uses RC4 as its stream cipher
• 802.11 leaves WEP implementation to vendors
10-5 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

Why WEP Was Chosen

Manufacturers rushed wireless LANs to market. In order to meet the 802.11 standard, manufacturers needed an encryption algorithm that met the following specifications:

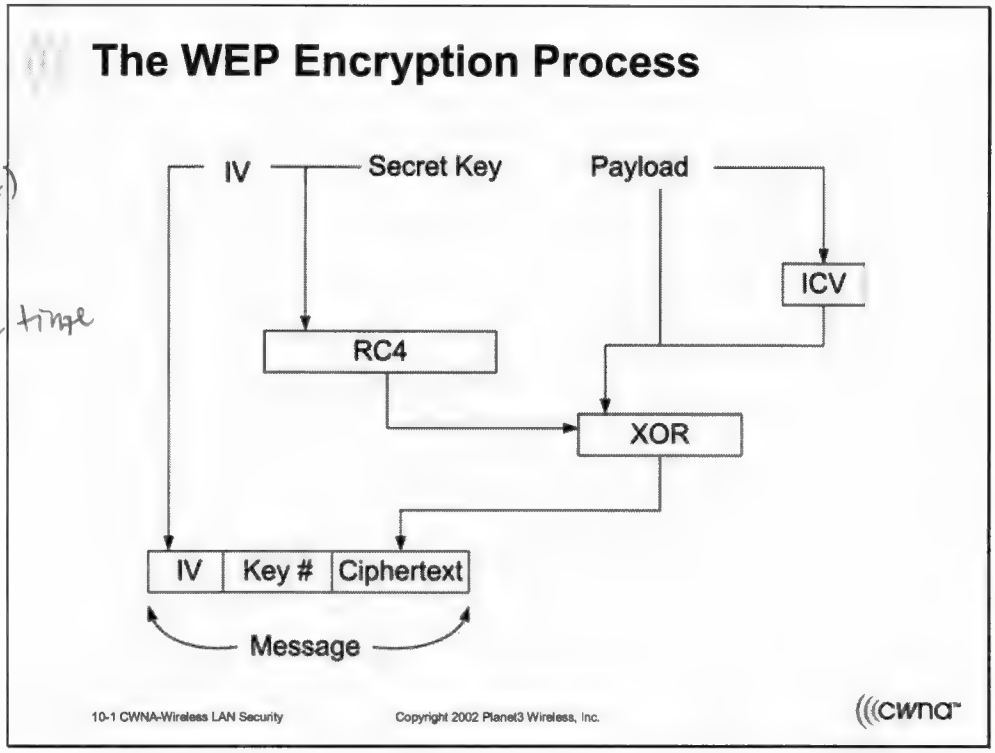
- Exportable – needed to be shipped outside the U.S.
- Reasonably Strong – cannot be cracked by the average non-cryptographer
- Self-Synchronizing
- Computationally Efficient – needed to encrypt/decrypt quickly on slower processors
- Optional

WEP uses a pseudo-random number generator (PRNG) and uses RC4 as its stream cipher. RC4 encrypts and decrypts quite quickly which makes it computationally efficient for the 802.11 requirements. RC4 was chosen because it was readily available and simple enough that most programmers could code it into software. RC4 meets the five requirements listed above.

The 802.11 standard leaves WEP implementation to vendors. There are no set methods for implementing WEP, as long as the five criteria listed above are met. No key distribution systems were defined as part of the 802.11 standard, so most vendors used static WEP keys for implementation. After products were released into the market, this solution was found to be unsecure.

LEAP (Cisco Proprietary)
- Change keys | WPA has the same function every time
- do it on the fly

TKIP
-



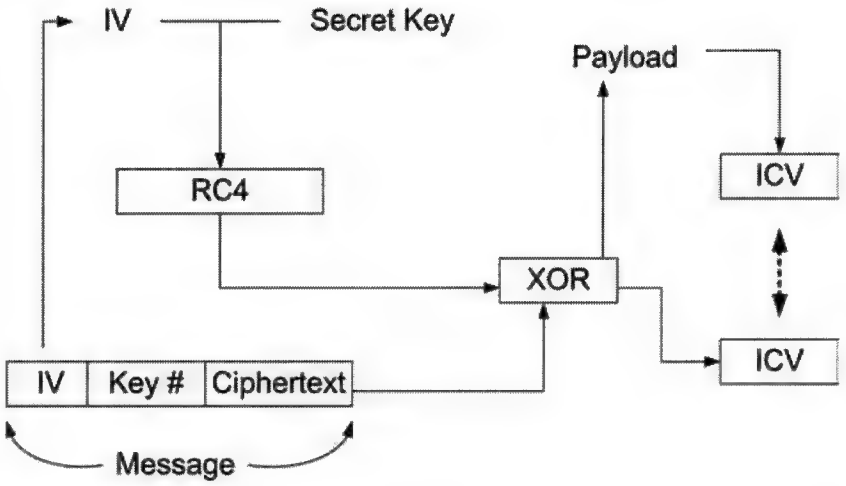
The WEP Encryption Process

When WEP is used, both the sender and receiver use the stream cipher to create identical pseudorandom strings from the known shared key (WEP key). The sender XORs the plaintext transmission with the stream cipher which produces ciphertext. The receiver then takes the shared key and stream cipher and reverses the XOR process to windup with plaintext again.

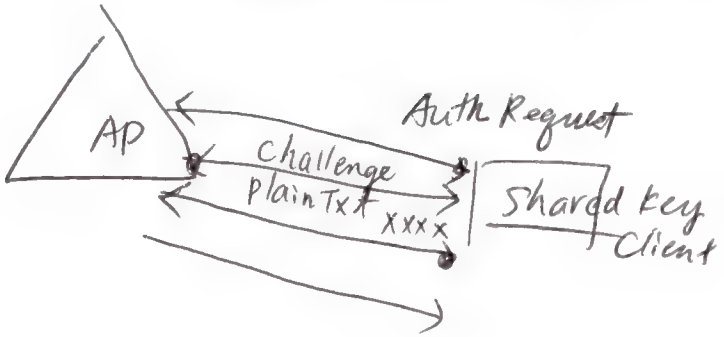
1. The plaintext traffic is sent through an Integrity Check algorithm (CRC-32 as specified by IEEE 802.11) which produces an Integrity Check Value (ICV).
2. The ICV is appended to the end of the plaintext message.
3. A 24-bit Initialization Vector (IV) is generated and prepended to the secret key.
4. This is then put into the RC4 algorithm to create a seed value for the WEP pseudo random number generator (PRNG).
5. The WEP PRNG next outputs the encrypting cipher-stream.
6. The encrypting cipher-stream is then run through a XOR process with the plaintext/ICV message. This produces the WEP ciphertext.
7. In the last step, the WEP ciphertext is then prepended with the plaintext IV and transmitted.

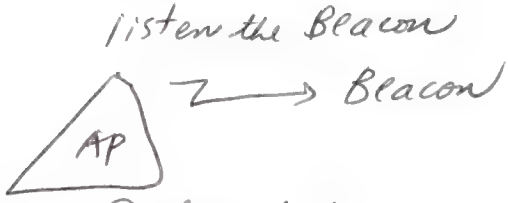
Copyright © 2003, Planet3 Wireless, Inc.

The WEP Decryption Process

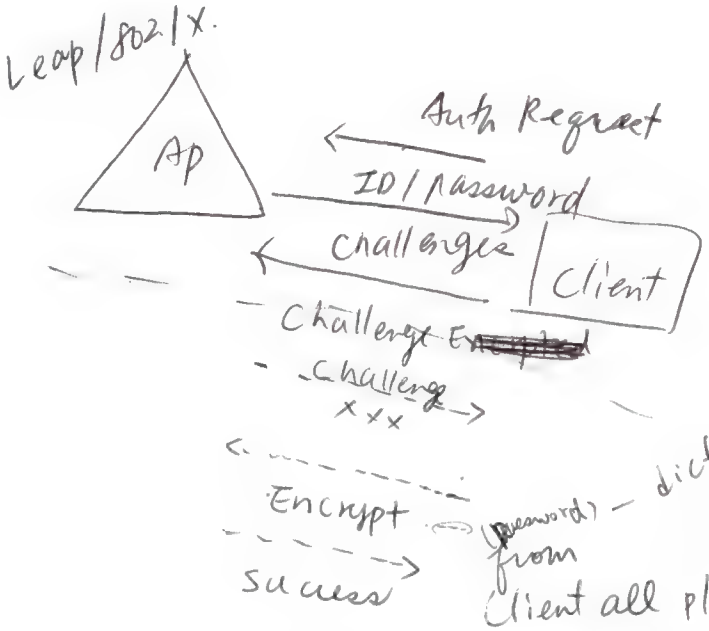


10-2 CWNA-Wireless LAN Security Copyright 2002 Planet3 Wireless, Inc. cwna

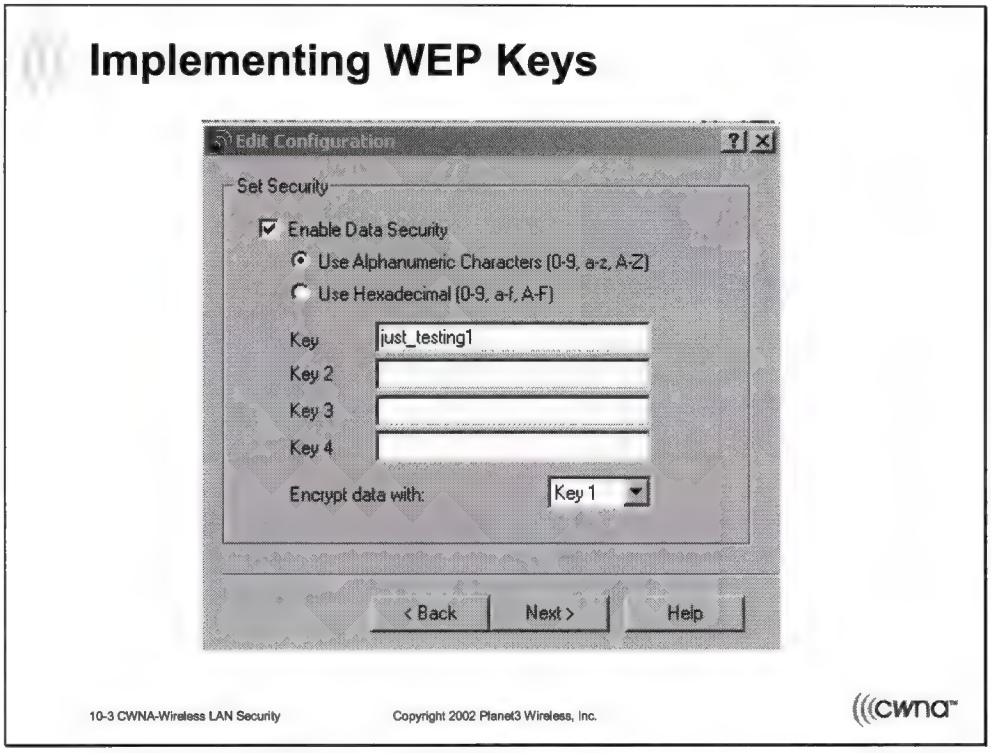




① check ACL
If you are not in ACL. then "ignore"
If you are in ACL then "accept"



(password) - dictionary attack
Can undo password.
from
Client all plain-Txt
from AP to sever
need to be encrypted

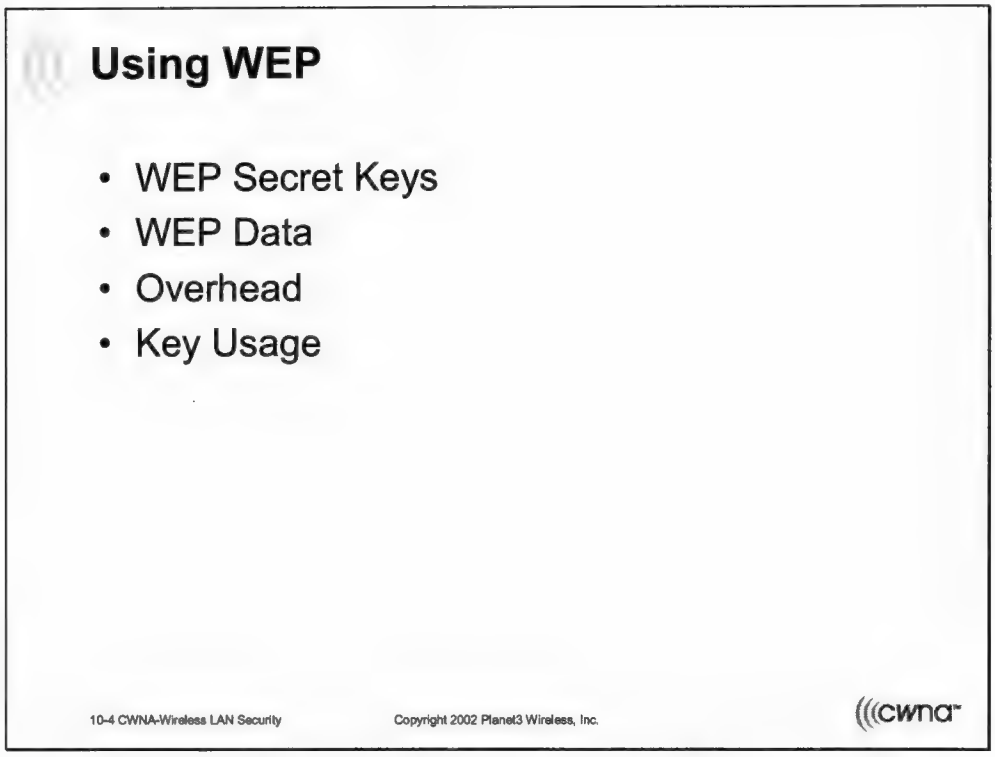


Implementing WEP Keys

As mentioned above, there are no standards for how the manufacturers of wireless LAN equipment implement their WEP solutions. Some vendors allow for use of Hexadecimal (Hex) or Alphanumeric (ASCII) WEP keys, whereas some vendors use only Hex or only ASCII WEP keys. These two types of key entry are convertible. There are many websites that provide ASCII-Decimal-Hexadecimal conversion charts.

Additionally, the 802.11b Wi-Fi™, standard only specifies 64-bit WEP encryption. Therefore, using 128-bit WEP encryption in a multi-vendor environment may or may not work, depending on the manufacturers.

Copyright © 2003, Planet3 Wireless, Inc.



Using WEP

Secret Keys

WEP secret keys are either 40-bit or 104-bit in length. The secret keys are concatenated with the 24-bit IV to form the WEP key (64-bit or 128-bit).

The WEP key is stored in the radio card's write-only firmware or in the Windows registry, depending on the manufacturer's driver software. In the firmware, the WEP key can be overwritten, but never viewed. In the Windows registry, some manufacturers store the WEP key encrypted, and others store it unencrypted.

WEP keys are used for authentication and data encryption.

Data Payload Encryption

When frames are transmitted over the wireless LAN using WEP, only the data payload is encrypted. Data payload is considered to be Layer3 information and above including Layer3 addresses. The Layer2 addresses are part of the frame header and are not encrypted. If headers were encrypted, all of the nodes on the network would need to decrypt every packet to decide if the packet was destined for them or not, which is not practical.

Beacons are not encrypted so that clients will be able to join the network and stay synchronized.

Overhead

WEP causes overhead that will significantly affect throughput. The data payload must be encrypted by the transmitting station and decrypted by the receiving station. CPU cycles must be used to perform encryption/decryption of packets.

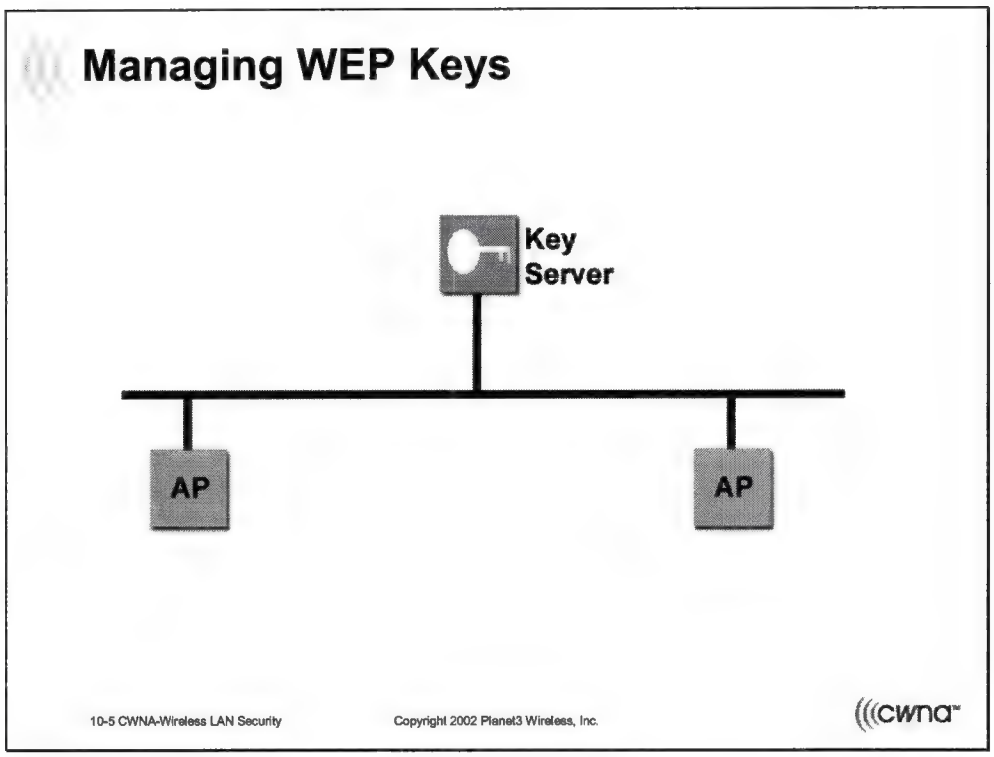
WEP can be implemented in hardware or software on the access point or bridge. On the client station, the main CPU is used for data encryption/decryption. Some manufacturers have separate processors in their access point designed to lighten the main CPU's load.

Key Usage

WEP keys are implemented on client stations, access points, bridges, workgroup bridges, etc. The WEP keys must match exactly at both ends of a connection for the data to be encrypted and properly decrypted.

Typically WEP clients and access points will only use their default WEP key, usually Key1, for sending. However, WEP clients and access points can respond to any of the four WEP keys that may be configured in their settings. In this way, clients and access points will be able to establish a communications session even if their default WEP keys are different.

Copyright © 2003, Planet3 Wireless, Inc.



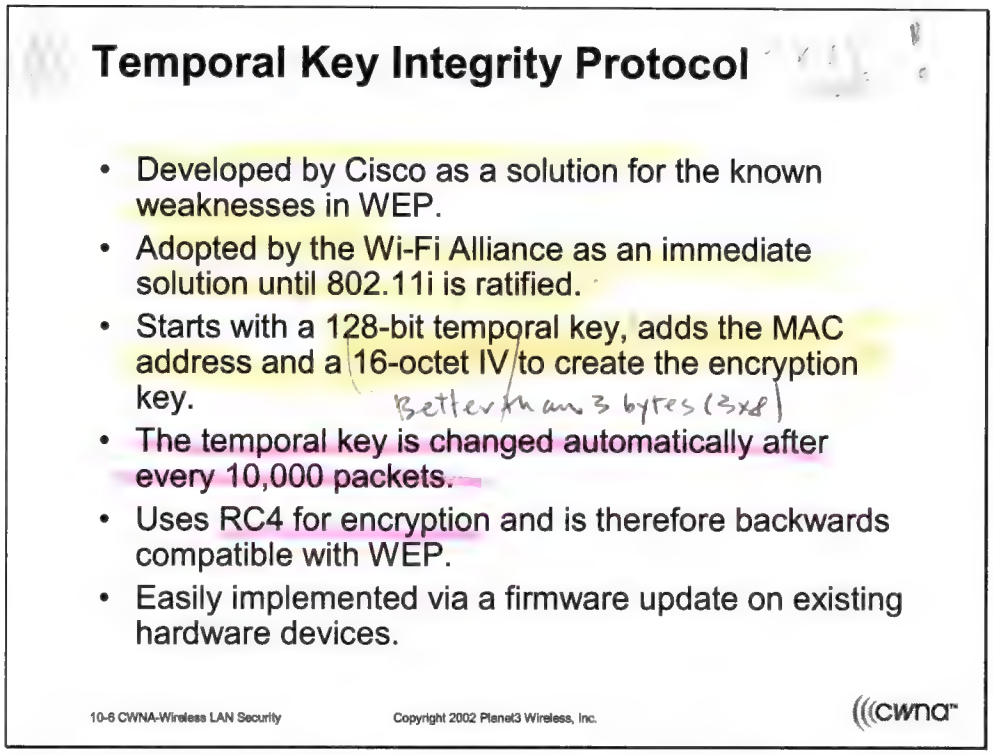
Managing WEP Keys

Static WEP keys can be difficult to administer. Centralized encryption key servers should be used if possible for a large wireless LAN implementation for the following purposes:

- Centralized key generation
- Centralized key distribution
- On-going key rotation
- Reduced key management overhead

Key generation can be done per-packet, per-session, or some other method depending on vendor implementation. Per-packet key generation will add very high network overhead. Key servers are typically RADIUS servers on the wired segment of the network.

Static WEP keys are fine for small implementations of wireless LANs such as small offices or home offices. When medium to large organizations implement static WEP keys, administration becomes unbearably time-consuming.


Temporal Key Integrity Protocol
• Developed by Cisco as a solution for the known weaknesses in WEP.
• Adopted by the Wi-Fi Alliance as an immediate solution until 802.11i is ratified.
• Starts with a 128-bit temporal key, adds the MAC address and a 16-octet IV to create the encryption key.
Better than 3 bytes (3x8)
• The temporal key is changed automatically after every 10,000 packets.
• Uses RC4 for encryption and is therefore backwards compatible with WEP.
• Easily implemented via a firmware update on existing hardware devices.
10-6 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
CWNA

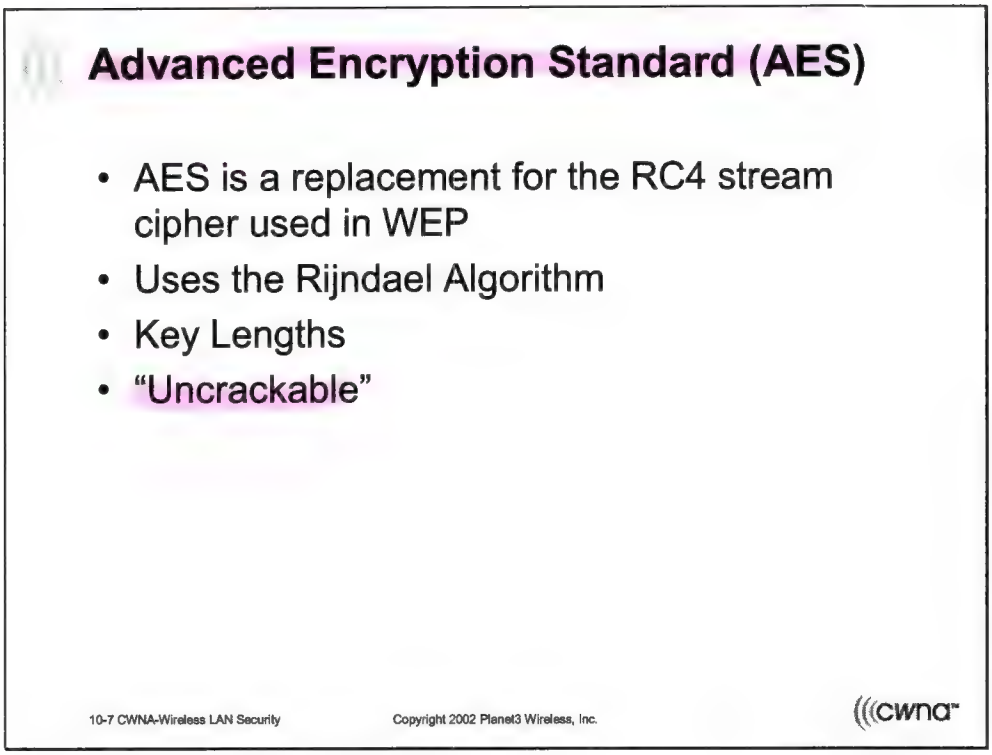
Temporal Key Integrity Protocol

TKIP (The temporal key integrity protocol) was initially referred to by many as WEP2, where in fact this is actually going to be AES. TKIP is a real solution that is available right now from many vendors as a firmware upgrade to existing Wi-Fi components and is expected to be in wide-spread usage by early 2003. Whereas WEP can use the same key to encrypt data all day long, TKIP does not.

TKIP starts out with a 128-bit temporal key that is shared amongst all clients and access points. This temporal key is then combined with a client's MAC address and then added to a very large 16-octet IV to produce the actual encryption key. By using this process, TKIP can effectively ensure that no two stations are using the same key stream for data encryption. RC4 is used to perform the encryption, as in WEP, thus TKIP is backwards compatible with WEP. To further ensure the security of TKIP on the network, the 128-bit temporal key is changed ever 10,000 packets--a period of time that can conceivably be reached in a very short time, under an hour in many cases.

Most hardware that is already in place can be upgraded to use TKIP through a standard firmware update. Access points running TKIP will still be able to service WEP-only clients due the aforementioned backwards compatibility, but this will introduce a security flaw into the network if utilized. TKIP looks to be a very promising solution until the 802.11i standard is ratified and included in new hardware devices.

Copyright © 2003, Planet3 Wireless, Inc.


Advanced Encryption Standard (AES)
• AES is a replacement for the RC4 stream cipher used in WEP
• Uses the Rijndael Algorithm
• Key Lengths
• "Uncrackable"
10-7 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

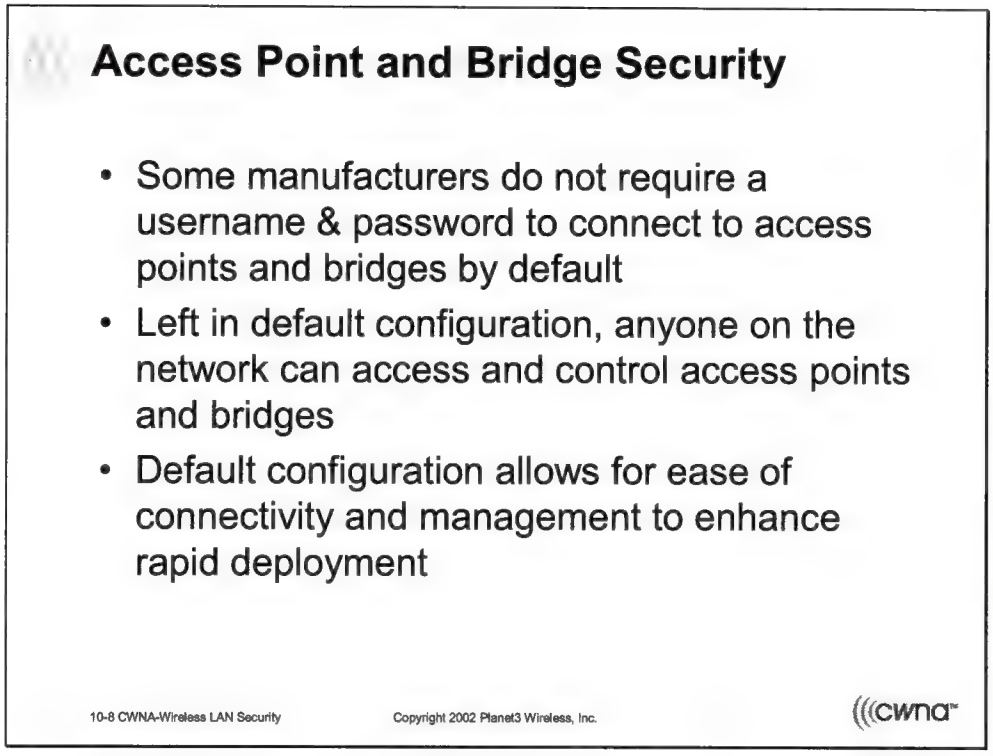
Advanced Encryption Standard

The Advanced Encryption Standard (AES) is likely to be the replacement for WEP. AES uses the Rijndael algorithm (pronounced "Rine Dale") whereas WEP uses RC4.

AES has key lengths specified at 128, 192, and 256 bits and is considered uncrackable by most cryptographers. However, very few algorithms to date have proven to be uncrackable, though many were thought to be so at one time or another.

The National Institute of Standards and Technology (NIST) chose AES for the Federal Information Processing Standard (FIPS). The IEEE 802.11i committee is considering use of AES for WEPv2.

AES requires more processing power for encryption/decryption which will mean that access points and bridges will require more processing power or separate encryption/decryption off-load processors in order to maintain throughput currently available in wireless LANs.


Access Point and Bridge Security
• Some manufacturers do not require a username & password to connect to access points and bridges by default
• Left in default configuration, anyone on the network can access and control access points and bridges
• Default configuration allows for ease of connectivity and management to enhance rapid deployment
10-8 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

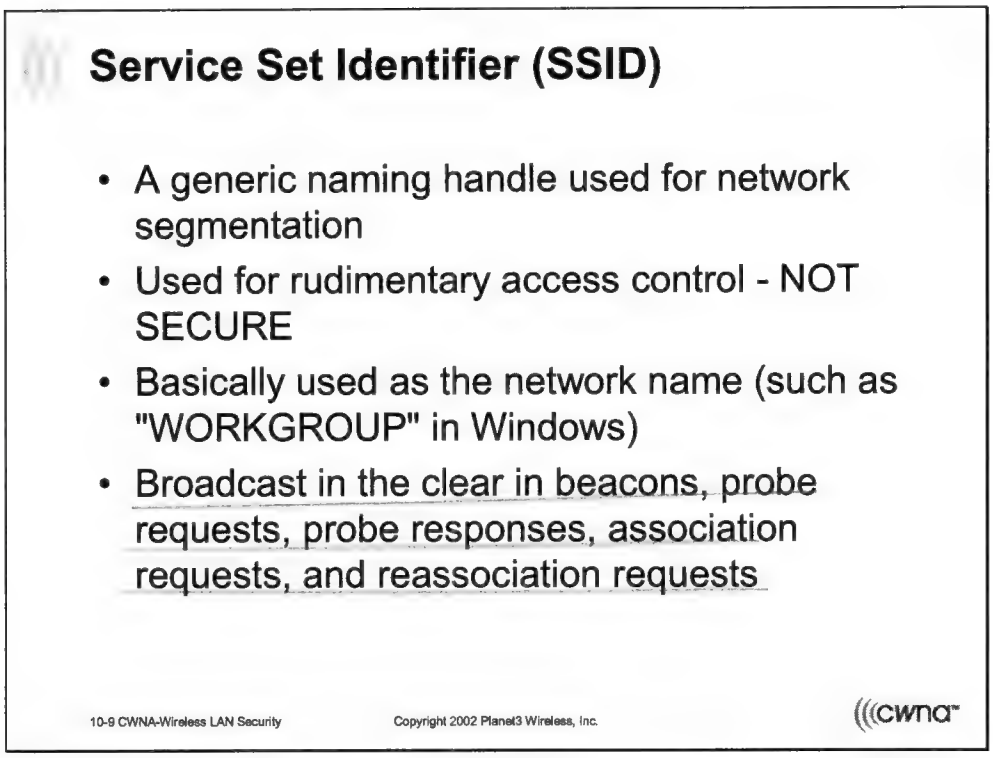
Access Point and Bridge Security

Some manufacturers do not, by default, require a username & password to connect to access points and bridges. Access points and bridges that are left in the default configuration could be controlled by anyone on the network. The default configuration of these devices was intended to allow for ease of connectivity and management to enhance rapid deployment.

When 802.11 compliant access points are received from the manufacturer, they are, by default, set to open system authentication with no use of WEP. If the default configuration is left unchanged, anyone can connect to the network and pass traffic, leading to unauthorized clients on the network.

It should be part of corporate security policy to change the default access point and bridge configuration during the staging process, prior to deployment. The default configuration settings are provided by the manufacturer for ease of deployment, but leaving them in this configuration is a security risk due to the fact that you are effectively placing rogue clients on your own network. These default settings are easily determined from the Internet and other sources and provide an open door for intruders to walk in without even having the need to place their own rogue on the network.

Copyright © 2003, Planet3 Wireless, Inc.


Service Set Identifier (SSID)
• A generic naming handle used for network segmentation
• Used for rudimentary access control - NOT SECURE
• Basically used as the network name (such as "WORKGROUP" in Windows)
• Broadcast in the clear in beacons, probe requests, probe responses, association requests, and reassociation requests
10-9 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
CWNA

Service Set Identifiers

A service set identifier (SSID) is a generic naming handle used for network segmentation. An SSID is not a security feature, and is only used for rudimentary access control and/or network segmentation. The SSID is used as a network name, very similar to the "WORKGROUP" name that is used in Windows by default and can be between 0 and 32 octets (bytes) in length. The SSID is broadcast in the clear in beacons, probe requests, probe responses, association requests, and re-association requests. Because it is broadcast in the clear, it can easily be picked up by anyone analyzing the network with a wireless network analyzer.

The SSID is sometimes stored in the Windows registry. Depending on the manufacturer, the SSID may be stored encrypted or not. For clarification, the acronyms SSID and ESSID (Extended Service Set Identifier) are synonymous. A network's BSSID (Basic Service Set Identifier) is the MAC address of the access point that will be used for relaying frames.

Common Default SSIDs

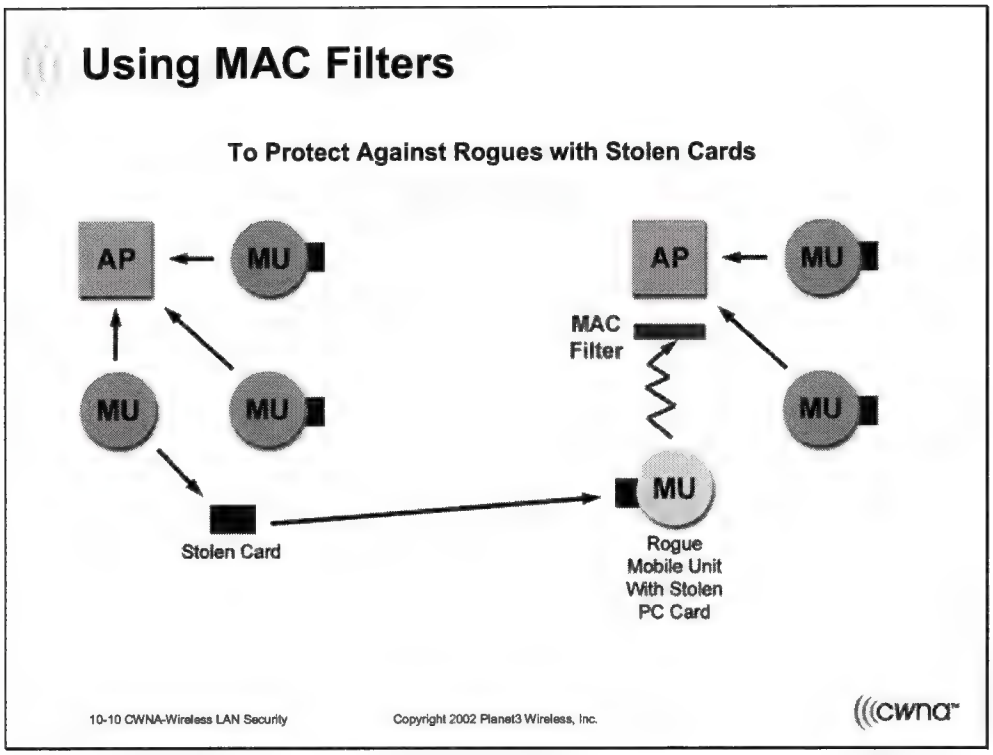
- Linksys – "linksys"
- Cisco – "tsunami"
- 3Com – "101"

Note A fairly comprehensive listing of default SSID's and WEP keys can be found at http://www.wi2600.org/mediawhore/nf0/wireless/ssid_defaults/. If the site is down, try http://www.80211bworld.com/links.php?op=visit&lid=14.

Closing the Network

One of the easiest ways that you can begin to increase the security of your wireless network is by closing it. By closing the network, you are disabling the broadcast of the SSID by configuring the AP to not respond to broadcast probes from clients. Clients wanting to associate with your Access Point will need to already know the correct SSID in order to become authenticated and associated. By closing the network, you prevent the popular NetStumbler (at least in its current version) from being able to see the network. NetStumbler sends out a broadcast probe approximately once per second, thus enabling it to locate open networks--ones that have not been configured not to respond to broadcast probes. Closing the network, however, is only a small part of an overall security solution and should not be considered enough to keep intruders out.

Copyright © 2003, Planet3 Wireless, Inc.



Using MAC Filters

Filtering

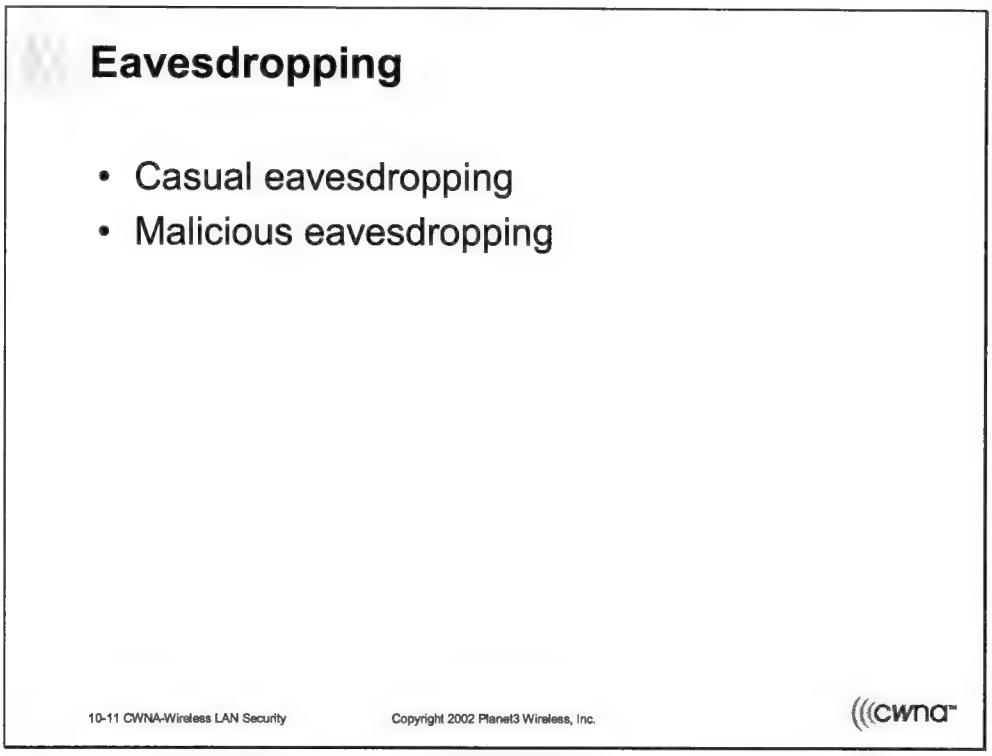
Filtering is the process of examining each frame to determine whether or not the frame meets a set of pre-defined rules or characteristics in order that a decision might be made as to the future processing of that frame. Filters can be created to allow or deny frames based on their meeting (or not meeting) a given list of criteria.

MAC Filters

Using MAC filters can result in slightly decreased throughput. MAC filters can be implemented in the access point, bridge, or in a RADIUS server.

MAC filters can be circumvented on access points. MAC addresses are broadcast in the clear even when WEP is used, so anyone analyzing the network can read the MAC address of a station.

Most wireless PC Cards permit the changing of the MAC address via software. When a valid MAC address is obtained, an intruder can take the stolen MAC address and configure the wireless card to use that address, and masquerade as the real station when the real user is not present on the network.



Eavesdropping

Casual Eavesdropping

Casual eavesdropping is a situation in which someone intercepts data transmissions without malicious intent. The individual is not looking to gain access to the network or to intercept sensitive data, but rather they just happen to be listening on the same frequency.

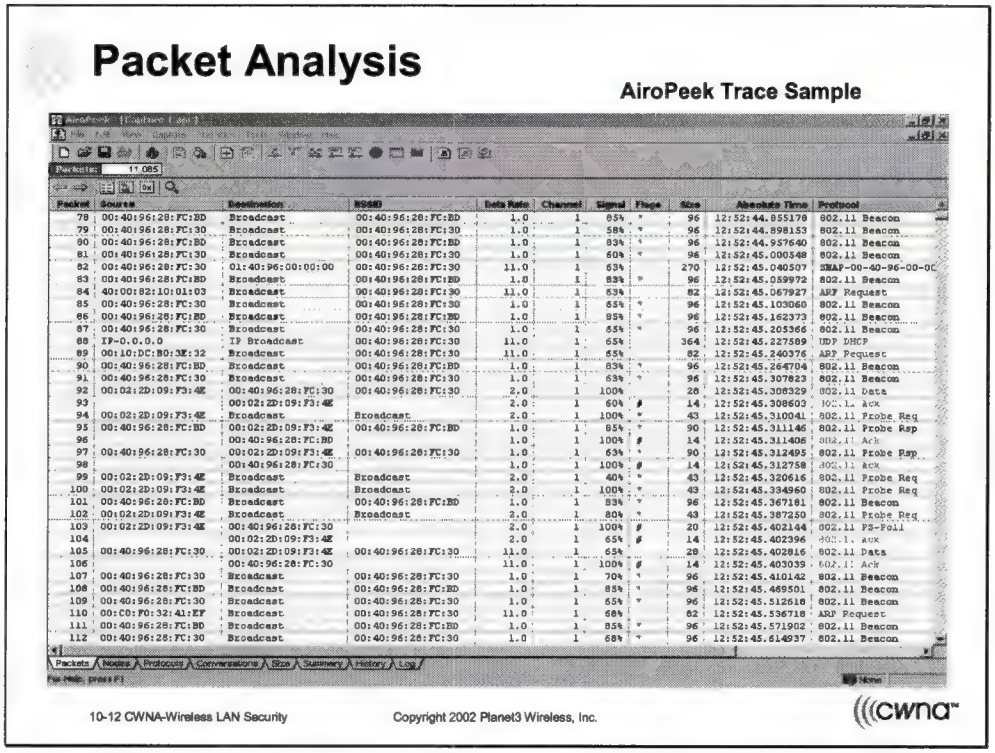
Individuals can "sniff" the network while being outside of the facility containing the wireless LAN. It is impossible to detect this type of "passive" attack since it requires no data frame changes. WEP is effective in reducing casual eavesdropping and will prevent an individual from gaining access in this case.

Malicious Eavesdropping

This type of intrusion can be done with inexpensive, off-the-shelf hardware and software. Data and WEP keys can be acquired with a wireless packet analyzer and easily obtained freeware hacking utilities. Once WEP keys, usernames, and passwords are captured, the user can masquerade as a legitimate user on the network without alerting the wireless network administrative staff.

To reduce the likelihood of malicious eavesdropping, the power output of access points should be kept to the minimum necessary. This type of administration will reduce the size of the access point's cell, thereby reducing the size of the area a hacker could be in to eavesdrop.

Copyright © 2003, Planet3 Wireless, Inc.



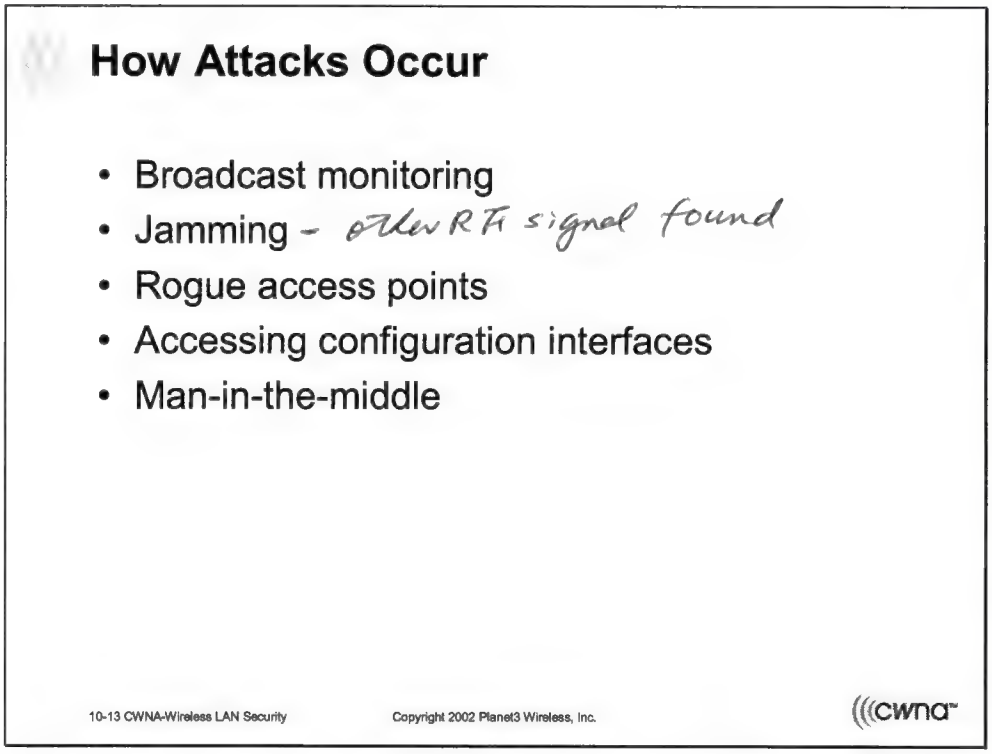
Wireless Packet Analyzers

The above illustration is an example of a packet analyzer trace. A wireless packet analyzer (such as WildPackets AiroPeek) allows an individual to place their wireless network card into "promiscuous" mode where it listens and records all packets being sent across the wireless segment of the network.

A wireless analyzer is useful for troubleshooting wireless LANs for problems and weaknesses in security. Analyzers capture information such as packet type, MAC addresses, IP or IPX addresses, data transmission channel and rate information, and signal strength.

Warning Hackers use wireless analyzers to obtain WEP information and address information that would be useful for gaining access into the network.

Copyright © 2003, Planet3 Wireless, Inc.



How Attacks Occur

Broadcast monitoring

If an access point is connected to a hub rather than a switch, any network traffic going across the hub will be broadcast over the wireless network. By connecting an access point into a switch, only broadcast frames from the wired LAN and unicast packets destined to the wireless LAN segment will be heard by the wireless clients.

If an access point is connected to a hub, rather than a switch, every node on both the wired and wireless segments of the network can hear all packets from and to all other stations. This configuration poses a security risk.

Jamming

Jamming is the act of imposing noise, data, interference, or any type of RF disruption onto the carrier frequencies being used for data transmission.

Jamming may be intentional or unintentional. The main solution to jamming would be to use a hardware or software spectrum analyzer to locate the RF interference source and then remove it.

Copyright © 2003, Planet3 Wireless, Inc.

The source of the jamming signal may be removable or non-removable. There may be a situation in which another wireless LAN in a nearby office is causing the problem. If jamming is caused by a non-removable source, a change in network frequency may be required.

Rogue Access Points

A Rogue access point is an unauthorized access point on the network. User groups within an organization that want their own wireless access may have added an access point. It is the responsibility of the wireless network administrator to find and either eliminate or control all such rogue access points that pose a security risk to the organization.

Rogue access points may also be placed onto a network by an attacker who is seeking to hijack users. Users connect to the rogue access point when it has a stronger signal (as perceived by the client station) than the legitimate access point. When users attempt to log in, they may unknowingly give away user accounts and passwords or other sensitive data to the perpetrator.

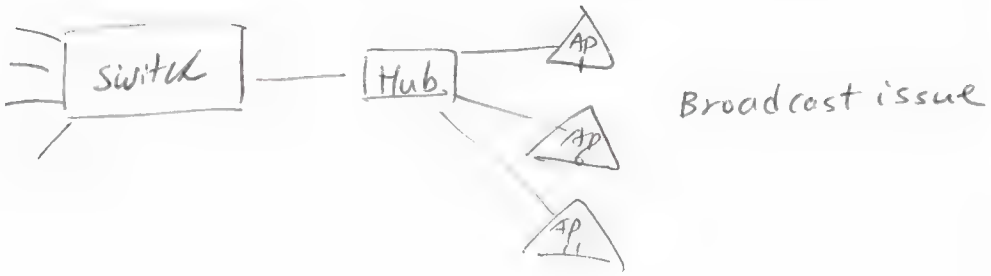
Accessing Configuration Interfaces

If an attacker can gain access to any of the following common configuration interfaces, the attacker can then control the access point or bridge:

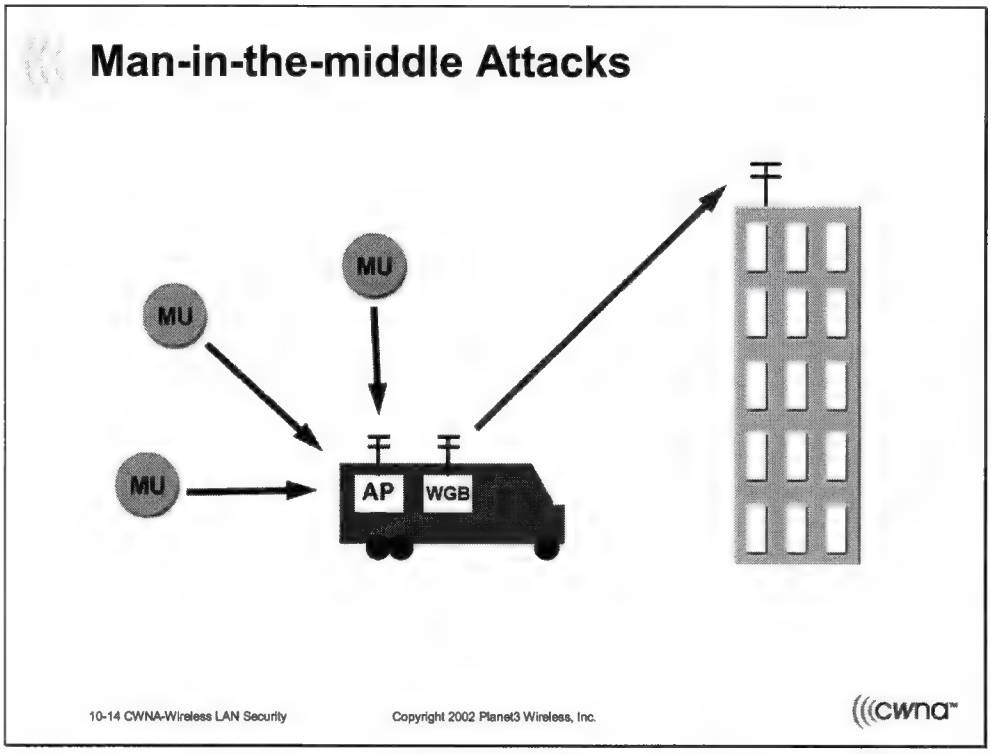
- SNMP
- Serial
- Telnet
- HTTP (Web)

With SNMP, obtaining the appropriate SNMP community string will allow an attacker to either listen to or control an access point or bridge. The common default community strings are "read", "write", "public", and "private".

Some wireless infrastructure devices that support built-in web servers (http) have no user authentication by default.



Copyright © 2003, Planet3 Wireless, Inc.

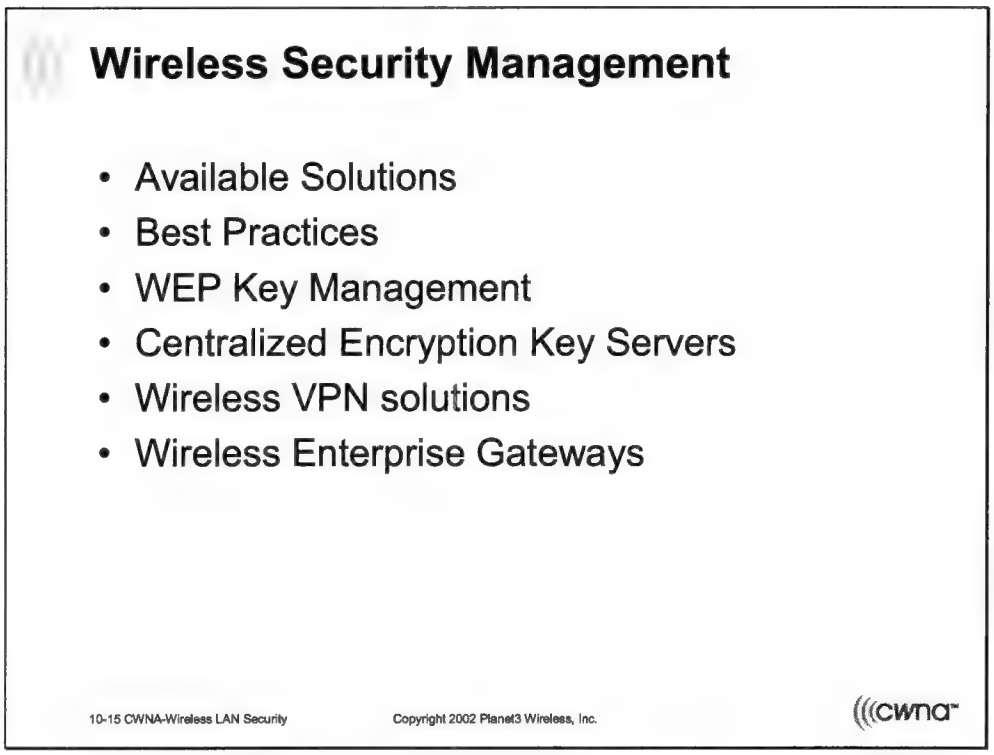


Man-in-the-Middle Attacks

Man-in-the-middle attacks occur when a user hijacks mobile nodes using an access point to allow unsuspecting users to authenticate / associate to the hijacker. Often a workgroup bridge is used in order to connect the users back into their corporate network from the rogue access point.

By performing this type of wireless network attack, hackers may be able to capture usernames, passwords, or other sensitive data that flows through the connection.

Copyright © 2003, Planet3 Wireless, Inc.



Wireless Security Management

Available Solutions

There are many types of wireless LAN security solutions on the market today. Currently, all of these solutions are proprietary. There are no security standards at present, but some IEEE standards are in progress as drafts. One such draft is the 802.1x, which incorporates use of the Extensible Authentication Protocol (EAP). Many vendors have begun basing their security solutions on this standard. Others in the market believe that the answer to wireless LAN security lies with VPN technologies. Both of these solutions have advantages and disadvantages, and both have a large market share.

There is no single "best" wireless LAN security solution, since each wireless LAN implementation is different. The best security solution is the one that meets the customer's needs, allows for growth and flexibility in management, and stays within the customer's budget. Some solutions are aimed at large enterprise organizations while others focus on small business or home environments. Other factors in choosing an appropriate wireless LAN solution might include:

- Difficulty of Implementation
- Overhead to network performance
- Scalability

Best Practices

For the most effective security, there should be a combination of strong encryption and user authentication. Using VPN technology, additional firewalls, and a Wireless Demilitarized Zone (WDMZ) can potentially be an expensive and difficult to implement solution. These factors might rule out their practical use in small wireless LAN configurations.

WEP Key Management

Using up to four WEP keys aids in the management of static key replacement. Using multiple WEP keys can also help with separating groups into 64- and 128-bit encryption for cards that do not support 128-bit WEP. It is also beneficial to use dynamic per-session or per-packet WEP key assignments instead of static keys in a larger wireless LAN implementation.

Centralized Encryption Key Servers

Centralized Encryption Key Servers should be used when use of static WEP keys becomes unmanageable.

Wireless VPN Solutions

With a virtual private network (VPN) solution, the access point can act as a stand-alone VPN server or many VPN/AP devices may be installed across the network. Clients must all load VPN software such as Microsoft's VPN client, which uses the point-to-point tunneling protocol (PPTP) to access the network.

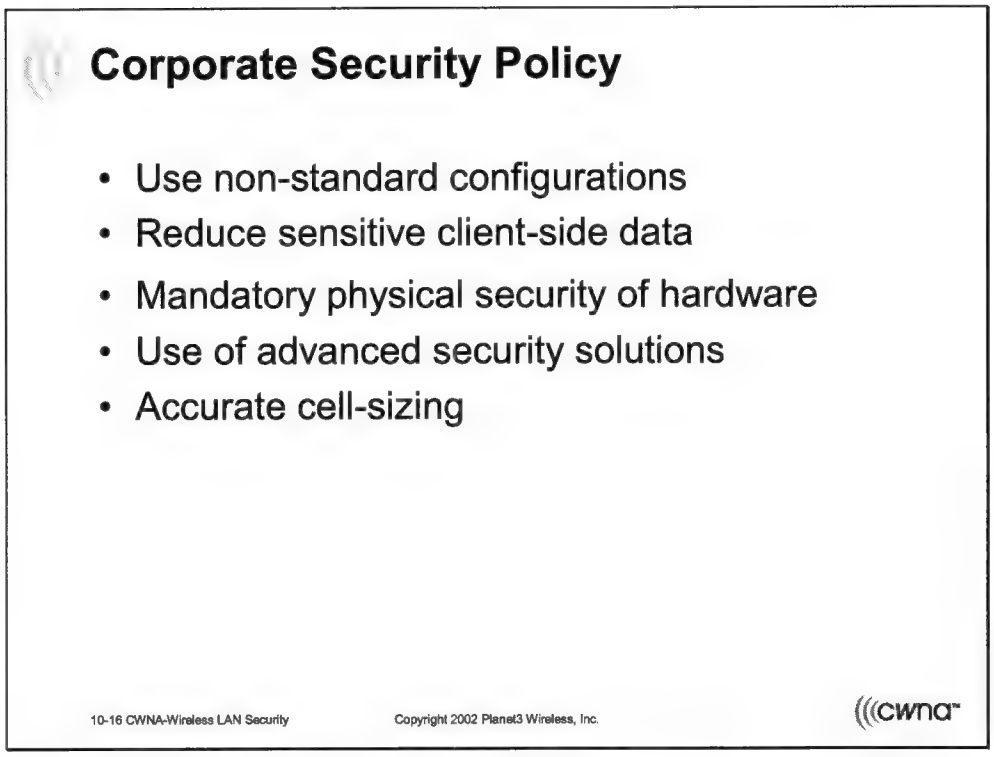
Wireless Enterprise Gateways

Enterprise gateways are a special adaptation of a VPN server for wireless networks. Most enterprise gateways support master/slave configurations so that when an administrator updates the master it will update the profiles on the slaves. This functionality simplifies and speeds up administration of the wireless network.

Since a user in close-proximity to the access point can easily saturate the wireless segment, a Denial of Service (DoS) situation can occur whether or not it was intentional. Enterprise gateways can solve this problem with role-based access control (RBAC) where types of users are assigned different classes of service (CoS). Users can be limited to the amount of data they can send through the gateway.

Copyright © 2003, Planet3 Wireless, Inc.

W3. securityfocus.com


Corporate Security Policy
• Use non-standard configurations
• Reduce sensitive client-side data
• Mandatory physical security of hardware
• Use of advanced security solutions
• Accurate cell-sizing
10-16 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

Corporate Security Policy

A corporate security policy for any type of network including wireless LANs is more important than the technology that is being used. The following outlines suggested measures that can be taken to secure a wireless LAN.

Use Non-standard Configurations

Prior to deployment, non-default configurations for access points and bridges should be implemented. The following should be configured as part of the staging process:

- Usernames and passwords of access points and bridges
- SNMP strings
- WEP keys

Reduce Sensitive Client-Side Data

Sensitive data is sometimes stored on client computers. Steps should be taken to reduce data exposure on client computers since client-to-client access is possible via the access point. This security step might not involve removing the data from the client computer, but rather installing personal firewall software or intrusion detection agent software onto the client computer.

Mandatory Physical Security of Hardware

Physical security of wireless LAN hardware should be mandatory and enforced as part of corporate security policy. Periodic inventorying of wireless LAN equipment can reduce stolen and misplaced hardware. If wireless network security is based on WEP, then a stolen wireless client device can constitute a breech of network security.

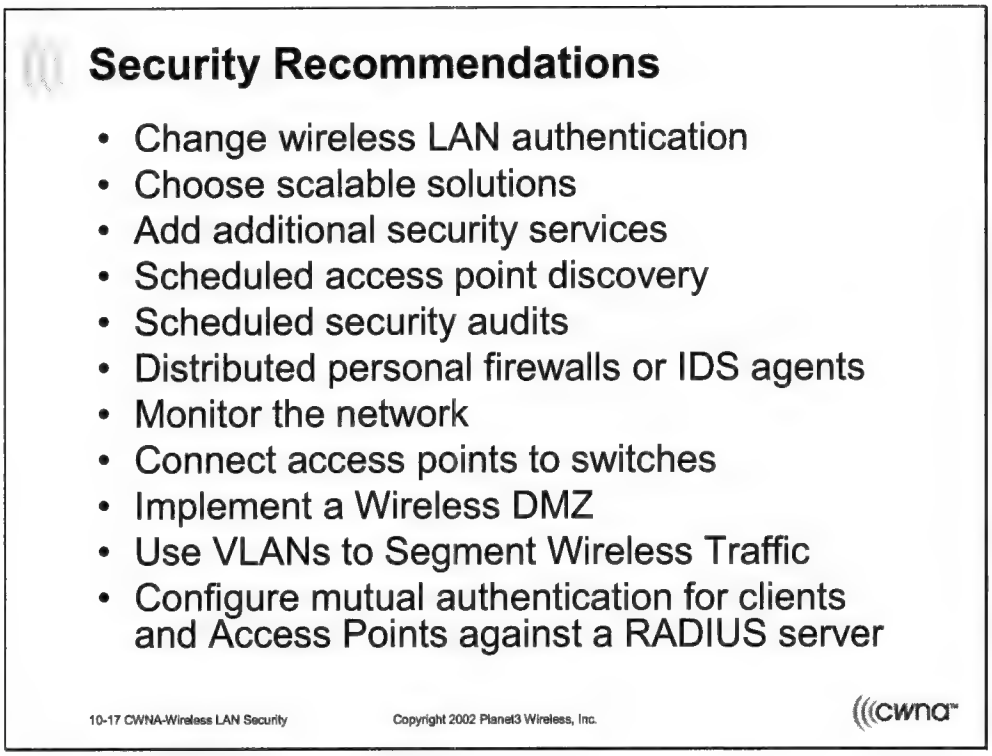
Use of Advanced Security Solutions

Use of advanced security solutions (beyond what is specified by the IEEE 802.11 standard) is strongly suggested. Many solutions types have been discussed in this section. It is a good idea for the student to be familiar with wireless security solutions currently on the market.

Accurate Cell-sizing

The size of the cell around the access points should be reduced to only cover the needed areas. Anything extending beyond the needed coverage areas constitutes a possible security weakness in the network. This concept applies to multi-floor or multi-tenant buildings, building-to-building links, and many other scenarios.

Copyright © 2003, Planet3 Wireless, Inc.


Security Recommendations
• Change wireless LAN authentication
• Choose scalable solutions
• Add additional security services
• Scheduled access point discovery
• Scheduled security audits
• Distributed personal firewalls or IDS agents
• Monitor the network
• Connect access points to switches
• Implement a Wireless DMZ
• Use VLANs to Segment Wireless Traffic
• Configure mutual authentication for clients and Access Points against a RADIUS server
10-17 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

Security Recommendations

The most important recommendation for wireless LAN security is not to rely solely upon WEP. Other recommendations to help build a secure environment for wireless LAN data networking are as follows.

Change Wireless LAN Authentication

Presently, user authentication is a wireless LAN's weakest link. No user authentication method is specified as part of the IEEE 802.11 standard. Wireless LAN authentication should be based on device-independent items such as usernames and passwords.

Choose Scalable Solutions

Choose a security solution that is scalable to meet the needs of the network. For example, a small office environment might benefit from using a VPN/access point solution in which users connect to the access point with VPN software built into the client's operating system. The user database could easily be built into the VPN/access point device eliminating the need for backend authentication systems.

For a large enterprise with hundreds or thousands of users, a large database of usernames, passwords, and network privileges must exist on a server. There must be some process in place to query this database, which necessitates the use of a solution such as RADIUS. This solution requires time, expertise, and is expensive to implement. Obviously, this solution would not be optimum for a small office environment, although it would work if implemented.

Add Additional Security Services

Use of VPNs, firewalls, intrusion detection systems (IDS), and client authentication with RADIUS can be added to the wireless network for additional security beyond what IEEE specifies in the 802.11 standard.

Scheduled Access Point Discovery

To assure there are no rogue access points on the network, periodically scheduled access point discovery should be completed to locate all access points that are on the network. Any access points not currently under the management control of the wireless network administrator should be removed from the network.

Scheduled Security Audits

Scheduled security audits (penetration assessments) should be done to determine poorly configured access points. By performing such audits regularly, the network administrator is assured on a regular basis that there are no gaps in wireless network security.

Distributed Personal Firewalls or IDS Agents

Distributed personal firewalls or IDS agents on clients can prevent intrusion into client machines and can notify network management of possible hacking activities. This solution is also helpful for locating and isolating virus problems.

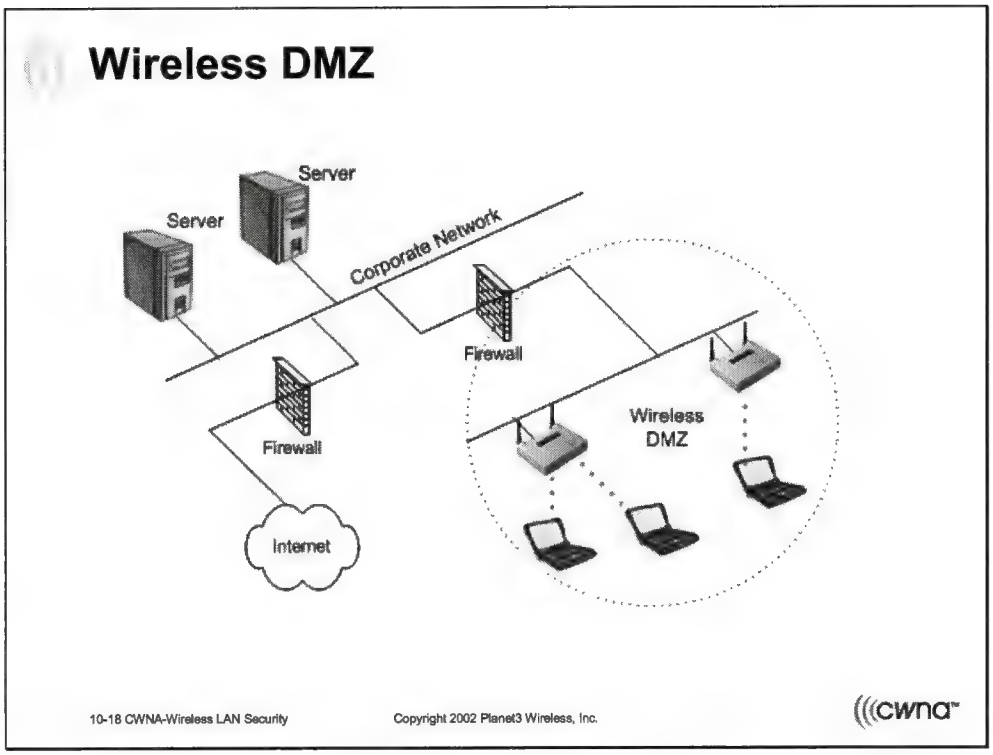
Monitor the Network

Monitoring of the wireless network for unauthorized access should be done on a regular basis. Network access logs will provide information on which users are logging in, from where, and how often. Anything out of the ordinary, such as a sales person logging into the network at 2AM on a Saturday night, is a sign something could be wrong.

Connect Access Points to Switches

Access points should be connected to switches, and never to hubs. Any network traffic going across the hub will be broadcasted over the wireless network.

Copyright © 2003, Planet3 Wireless, Inc.



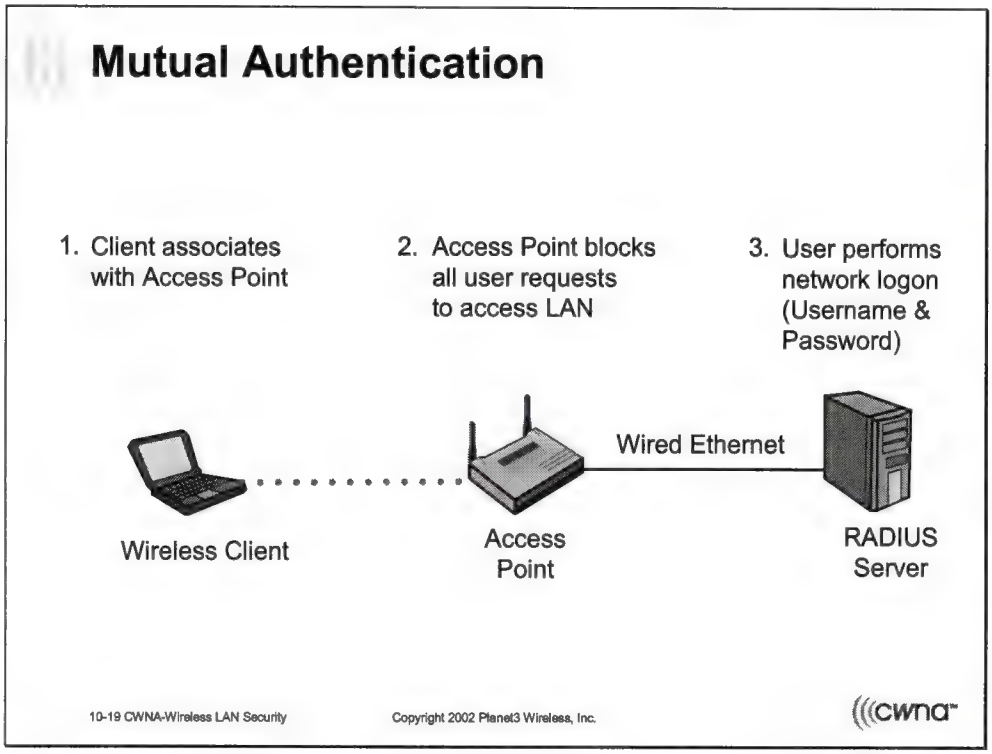
Implement a Wireless DMZ

Use of a wireless DMZ (WDMZ) should be considered when installing medium to large enterprise implementations of wireless LANs. Access points should always be considered untrusted devices. Access points should be grouped and segmented from the network core by a firewall-like device for optimum security.

Use VLANs to Segment Wireless Traffic

The use of VLANs can help keep wireless traffic isolated from the trusted network even when the wired network is used to connect the access points. VLANs create virtual LAN segments that can overlay the wired network, allowing traffic only between ports explicitly defined as belonging to a particular VLAN. Creating one (or more) VLANs for the wireless network and one (or more) VLANs for the trusted (wired) network will keep each network's traffic separate, even though they traverse the same physical connections.

The wired and wireless VLANs are connected using a router, firewall, or enterprise wireless gateway. This creates a single connection between the wired and wireless networks, allowing for the ability to track, log, and limit wireless clients to the corporate network.


Mutual Authentication
1. Client associates with Access Point
2. Access Point blocks all user requests to access LAN
3. User performs network logon (Username & Password)
Wired Ethernet
Wireless Client
Access Point
RADIUS Server
10-19 CWNA-Wireless LAN Security
Copyright 2002 Planet3 Wireless, Inc.
cwna

Configure Mutual authentication for clients and Access Points against a RADIUS Server

It is possible that a rogue client could be placed on your network configured with the correct SSID and subsequently hijack your clients, thus creating a DOS situation for them. The clients are prevented from reaching the real network and thus are being denied service. By implementing a mutual authentication solution using a RADIUS server with the Access Point between the client and the RADIUS server, you can provide a means for both the client and the network to verify each other's identity. The client authenticates the network via a RADIUS server; likewise, the RADIUS server authenticates the client. The two sides of the authentication scheme are decoupled on separate secure channels, with the access point in the middle. Many mutual authentication solutions have been developed which can be quickly and easily implemented to greatly enhance the security of your wireless network design. Solutions from Cisco (LEAP) and Funk Software have been well tested and ready to implement in a network of any size.

Copyright © 2003, Planet3 Wireless, Inc.

Chapter

11 Site Survey Fundamentals

Objectives

Upon completion of this chapter you will be able to:

- Understand the need for a Site Survey
- Determine the business needs for the Wireless LAN
- Locate and avoid RF interference
- Determine RF coverage contours
- Locate the appropriate places for hardware installation
- Document Site Survey results on the appropriate forms
- Define and create an RF Site Survey Report

11-2 CWNA- Site Survey Fundamentals Copyright 2002 Planet3 Wireless, Inc. ((cwna™

Chapter Content

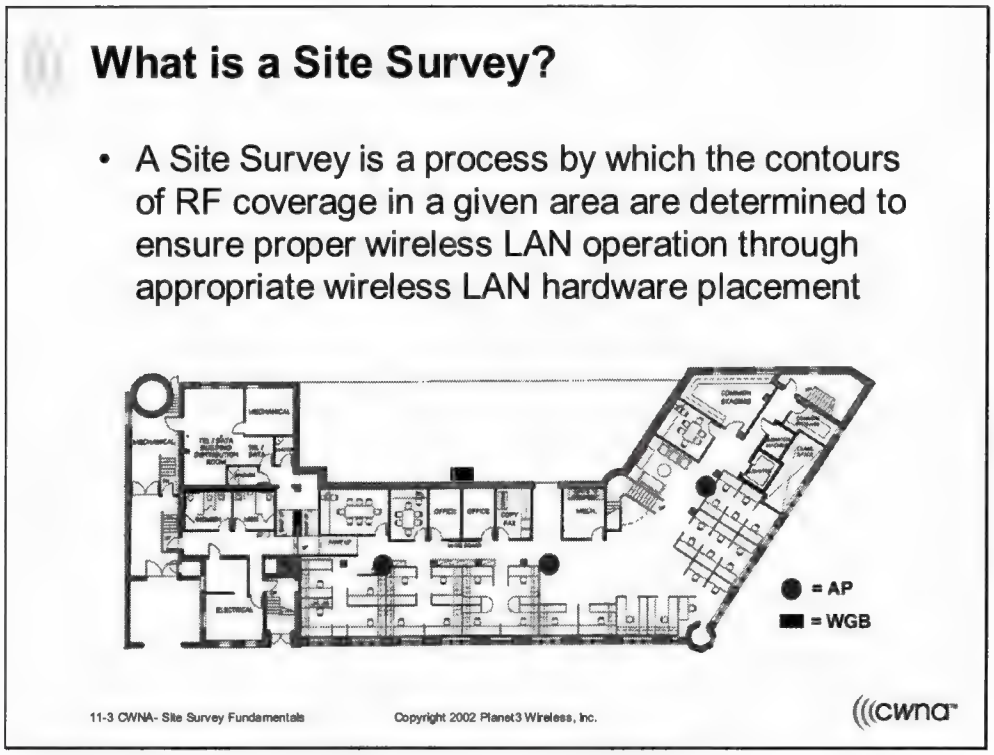
Before installing wireless LAN hardware, it must be determined that there will be adequate radio wave coverage throughout the facility and that no unforeseen RF interference will wreak havoc on the system to be installed. The importance of performing an RF site survey before the installation of a wireless LAN cannot be emphasized enough.

This chapter discusses the steps involved in performing a site survey. The steps provided in this chapter will ensure a more successful implementation of a wireless LAN.

The chapter outline follows:

- What is a Site Survey?
- Interviewing Network Management
- Locating RF Interference
- Determining Contours of RF Coverage
- Locating Hardware Installation Points
- Documenting Installation Issues
- Site Survey Reporting

Copyright © 2003, Planet3 Wireless, Inc.

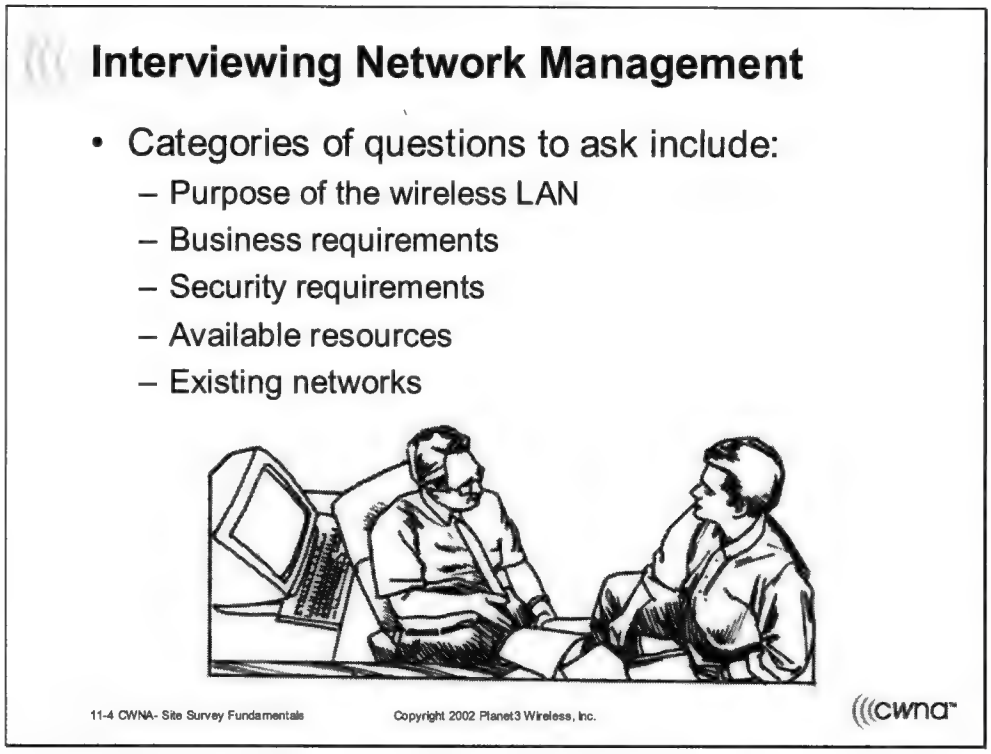

What is a Site Survey?
• A Site Survey is a process by which the contours of RF coverage in a given area are determined to ensure proper wireless LAN operation through appropriate wireless LAN hardware placement
= AP
= WGB
11-3 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

What is a Site Survey?

Site surveying involves analyzing a site from an RF perspective and discovering what kind of RF coverage a site needs in order to meet the business goals of the customer. During the site survey process, the surveyor will ask many questions about a variety of topics, which are covered in this chapter. These questions allow the surveyor to gather as much information as possible to make an informed recommendation about what the best options are for hardware, installation, and configuration of a wireless LAN.

A site survey is an attempt to define the contours of RF coverage from an RF source (an access point or bridge) in a particular facility. Many issues can arise that prevent the RF signal from reaching certain parts of the facility. For example, if an access point were placed in the center of a medium-sized room, it would be assumed that there would be RF coverage throughout the room. This is not necessarily true due to phenomena such as multipath, Near/Far, and hidden node. There may be "holes" in the RF coverage pattern due to multipath or stations that cannot talk to the network due to Near/Far.

Though a surveyor may be documenting the site survey results, another individual (possibly the RF design engineer) may be doing the site survey analysis to determine best placement of hardware. Therefore, all of the results of the entire survey are to be documented. The surveyor and the designer may be the same person, or in larger organizations they may be different people. Organized and accurate documentation by the site surveyor will result in a much better design and installation process. Appendix A contains some sample site survey forms.



Interviewing Network Management

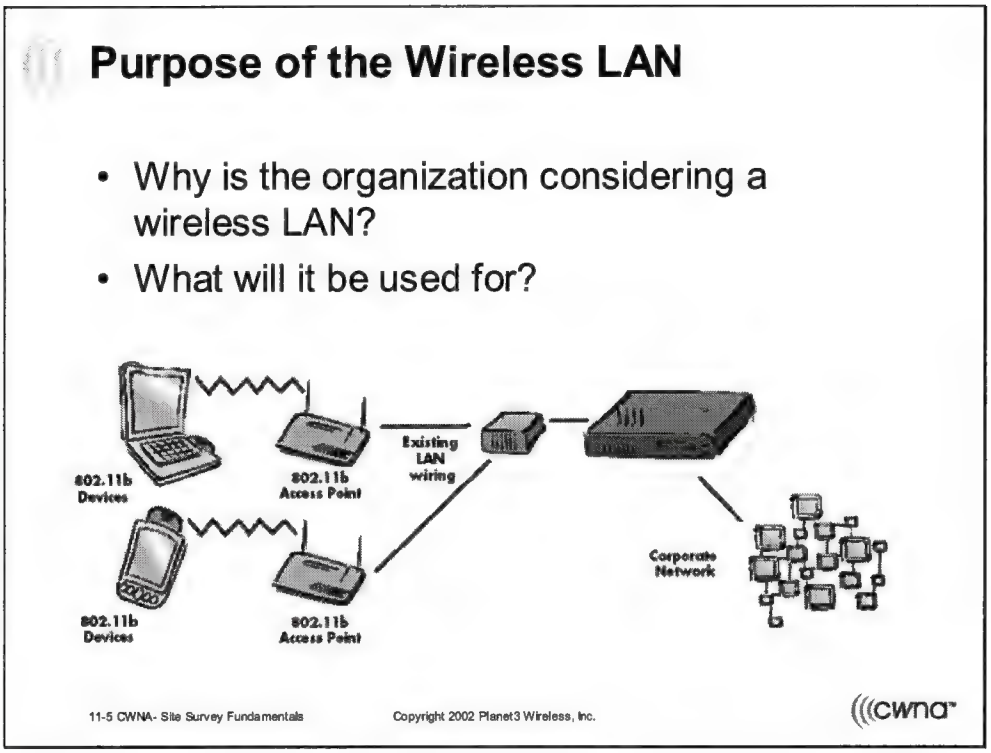
Interviewing the network manager is the first step in the site surveying process. The network manager will indicate what needs to be done, why the site survey is needed, and what business requirements must be met, and much more.

There are many questions that need to be asked of the network manager. These questions can be divided into the following categories:

- Purpose of the wireless LAN
- Business requirements
- Security requirements
- Available resources
- Existing networks

Each of these categories is discussed in the following pages.

Copyright © 2003, Planet3 Wireless, Inc.



Purpose of the Wireless LAN

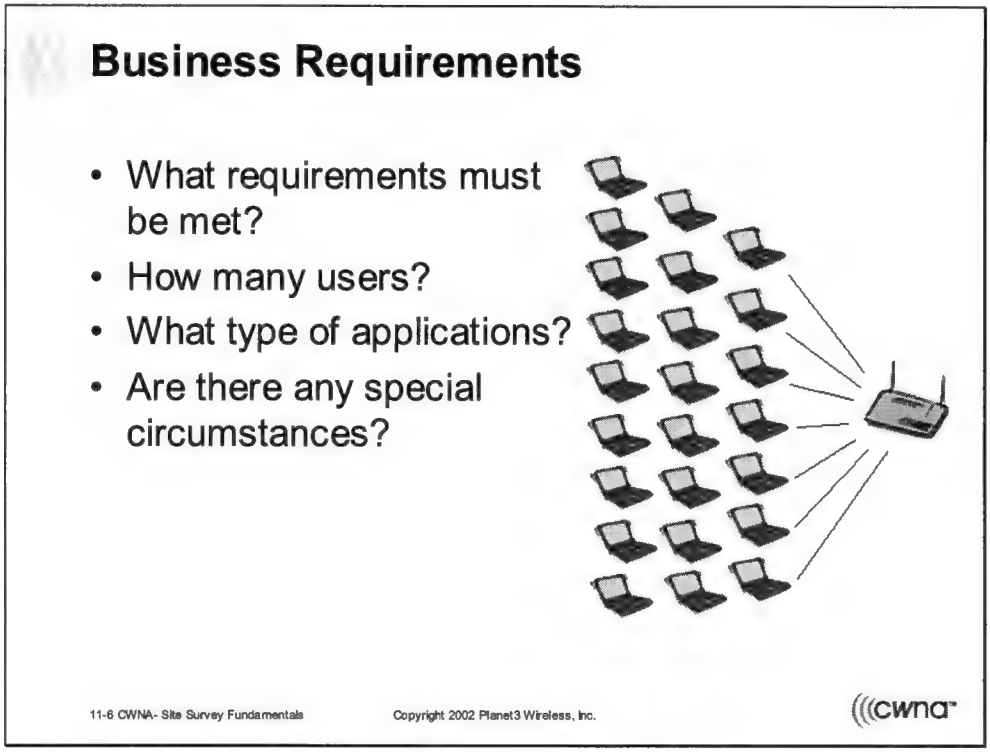
Questions the network manager should be asked about the purpose of the wireless LAN include:

Why is the organization considering a wireless LAN?

If an organization is considering installation of a wireless LAN, someone must have made the recommendation for a particular reason. This person, usually the network manager, should define why the organization believes a wireless LAN will provide an appropriate solution to the particular needs of the organization.

What is the purpose of the wireless LAN?

Uses of the wireless LAN must be discussed. Recommending a high-speed 802.11a installation for an organization that is only using a few wireless PDAs would be a poor judgment, so the needs of the users must be known. As much information as can be gathered will be helpful in understanding how the wireless LAN is to be used. This information gathering may require interviews with some network users as well as network management.


Business Requirements
• What requirements must be met?
• How many users?
• What type of applications?
• Are there any special circumstances?
11-6 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Business Requirements

Questions the network manager should be asked about the business requirements of the wireless LAN include the following.

What are the business requirements that the wireless LAN must meet?

The necessary speed, range, and throughput per user must be known so that when the site survey is given to the RF design engineer, the design engineer can create a solution that is cost effective and meets the needs of the users. Cost is another factor that would fit into this category of questioning. Most companies are broken into several departments such as engineering, accounting, marketing, human resources, etc. Each department type may have different uses of the wireless LAN in their area.

Copyright © 2003, Planet3 Wireless, Inc.

How many users are typically in a given area?

An understanding of how many users will be located in a given area is required to calculate how much throughput each user is going to get. This information is also used to decide on which technology, such as 802.11b or 802.11a, would be most well suited to the needs of the users. If the network manager is not able to provide this information, the person doing the site survey will need to interview the actual users to be able to make an informed decision. Different departments within an organization will have different numbers of users. It is important to understand that the needs of one part of a facility might be different from the needs of another part of a facility.

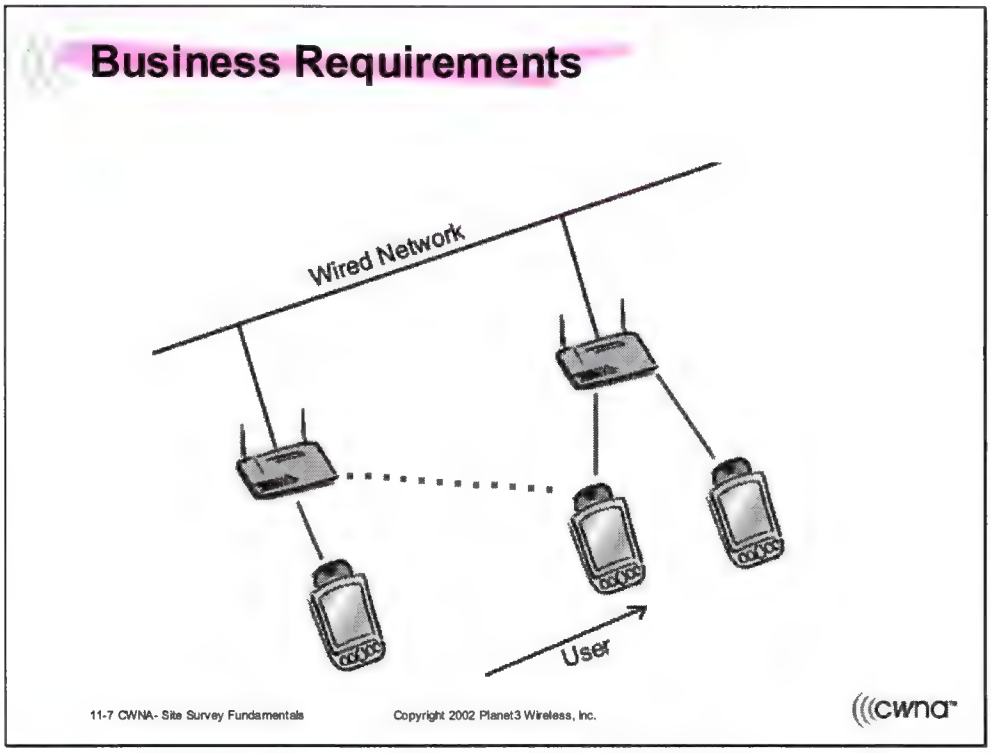
What type of applications will be used with the wireless LAN?

Find out if the network is being used to transmit non time-sensitive data only, or time-sensitive data such as voice or video. The data may also be communicated through connection-oriented applications such as telnet. High bandwidth applications such as voice or video will require higher throughput per user than an application that makes infrequent network requests. Connection-oriented applications will need to maintain connectivity while roaming. Analyzing and documenting these application requirements before the site survey will allow the site surveyor to make more informed decisions when testing areas for coverage.

Are there any non-typical times in which network needs may change for a particular area?

Changes in network needs could be something as simple as more users being on a particular shift or something as difficult to discover as seasonal changes. For example, if a building-to-building bridge link were being discussed, it could be that it is winter and the trees are without leaves. In the spring, trees will fill with leaves possibly causing problems with the link.

Copyright © 2003, Planet3 Wireless, Inc.

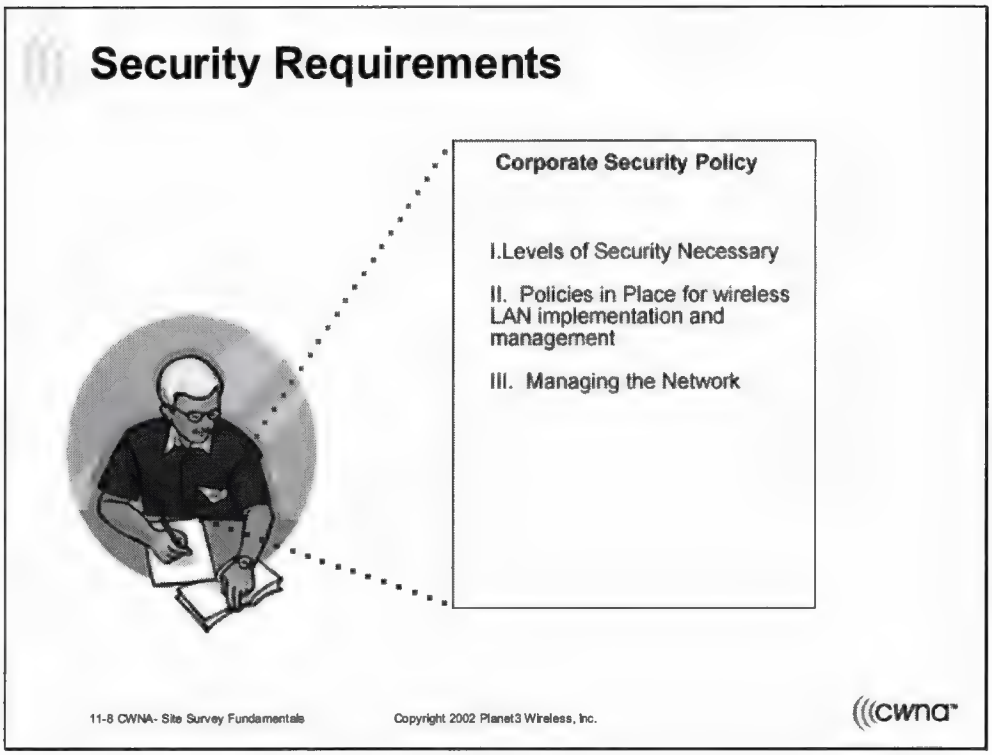


What mobility or roaming coverage is necessary?

Users may want to roam indoors, outdoors, or both. Roaming may also have to incorporate crossing of router boundaries, maintaining VPN connectivity, and other complex situations. If this were the case, it would be important for the site surveyor to document these facts so that the wireless network design engineer would have all of the facts before presenting a solution to the customer.

There may be areas within or around a facility that require special connectivity solutions, due to blockage of RF coverage or to special security requirements, in order to provide roaming.

Copyright © 2003, Planet3 Wireless, Inc.


Security Requirements
Corporate Security Policy
I.Levels of Security Necessary
II. Policies in Place for wireless LAN implementation and management
III. Managing the Network
11-8 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Security Requirements

Gathering as much information as possible on the security requirements is important. While this information does not become part of the site survey report, it can be used for subsequent reporting such as with consulting reports and security audits.

Questions the network manager should be asked about the security requirements of the wireless LAN include the following.

What level of security is necessary?

Customers may have very strict demands for data security, or in some cases, no security may be required.

It should be explained to the customer that WEP should not be the only wireless LAN security method used because WEP can be easily circumvented. Briefly educating the customer on available security options is an important step in getting started with a site survey. A discussion with the customer will provide them enough information to feel informed and will allow them to better understand the solutions likely to be presented by the design engineer. After this discussion, the customer may likely have several questions involving wireless network security that may aid the site surveyor in properly documenting the customer's business needs.

What corporate policies are in place regarding wireless LAN security implementation and management?

The network manager may not have any security policies other than users having passwords on sticky notes on the bottom of their computer's keyboard. If the customer already has a wireless LAN in place, the existing security policies should be reviewed before the site survey is started.

If corporate security policies relating to wireless LANs do not exist, ask questions about security requirements regarding installations of wireless LANs.

During the design phase (design is not part of the site survey itself), the RF design engineer could include a security report detailing security suggestions for this particular installation. The network administrator could then take this information and form a corporate policy based on sound suggestions.

Security policies may differ slightly between small, medium and enterprise installations, and can sometimes be re-used. There are general security practices that are common to all installations of wireless LANs. These policies may also include how to manage the wireless network once it is installed.

Copyright © 2003, Planet3 Wireless, Inc.

Available Resources
• Are blueprints available?
• Are any previous site survey reports available?
• Is a badge required?
• Are the wiring closets accessible?
11-9 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Available Resources

Questions the network manager should be asked about the available resources needed for the site survey include the following.

Are facility blueprints available (electronic or printed)?

Among the first items to request from a network manager are blueprints or some kind of map showing the layout of the facility. Without the official building or facility schematics, a diagram must be created that shows the dimensions of the areas, the offices, where the walls are located, network closets, power outlets, etc.

Creating such a drawing can be a time-consuming task. If it is necessary to manually create such a document, simple things like notebook paper with grid lines are helpful in being efficient as the site survey is performed. This information can later be put into Visio, AutoCAD, or other such applications for professional presentation to the customer as part of the RF site survey report.

Are there any previous site survey reports available?

If a company has previously done a site survey at an earlier date, having that site survey available can cut down on the time it takes for the new survey to be completed. Be sure that the previous report does not bias the decisions made regarding the current site survey.

Is a facilities escort or security badge required?

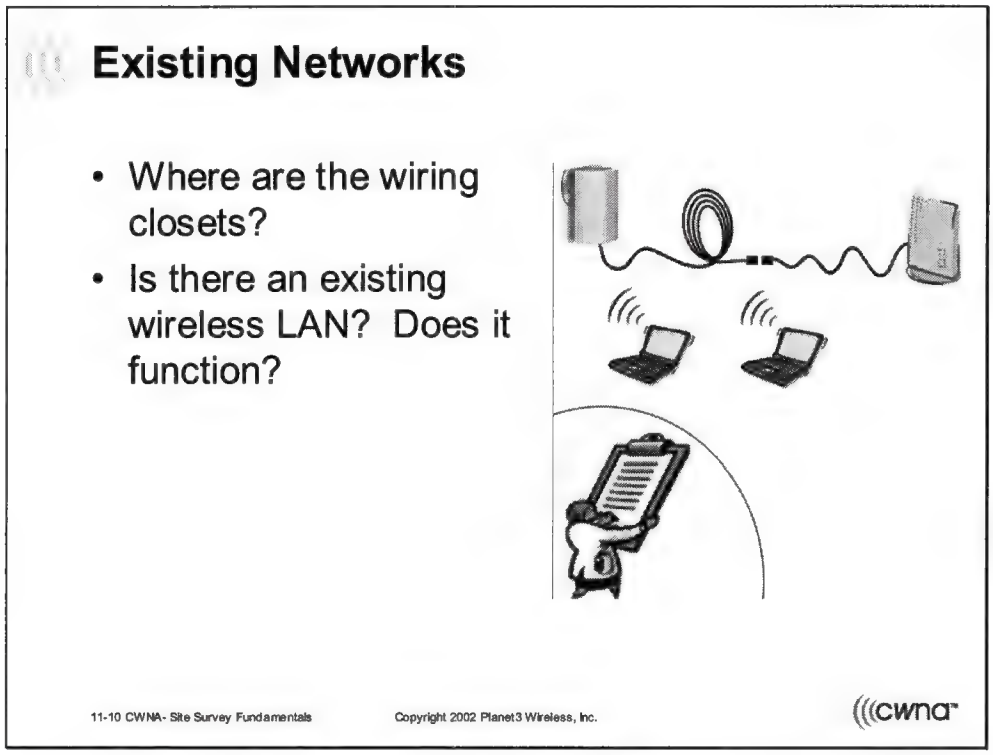
A security badge or an escort may be required to move throughout the facility freely. When performing a site survey, every square foot of the facility is usually covered in order to be able to answer all of the questions needed to define the RF coverage.

Note It has been said that RF site surveying is 90% walking, and 10% surveying. This is usually true, so one should wear very comfortable shoes and make sure that an escort (if necessary) has plenty of time while the survey is being performed.

Is physical access to wiring closets and the roof available if needed?

Physical access to both the roof and to wiring closets may be needed to determine antenna placement and network connection points.

Copyright © 2003, Planet3 Wireless, Inc.


Existing Networks
• Where are the wiring closets?
• Is there an existing wireless LAN? Does it function?
11-10 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Existing Networks

Questions the network manager should be asked about the existing wireless LANs might include the following.

Where are the network wiring closets located?

It is not uncommon to find that what seems like the most appropriate location for installing an access point ends up being too far from a wiring closet to allow for upstream network connectivity. Knowing where these wiring closets are ahead of time will prevent much wasted time. Locations of these wiring closets should be documented on the network topology map, blueprints, or other facility maps.

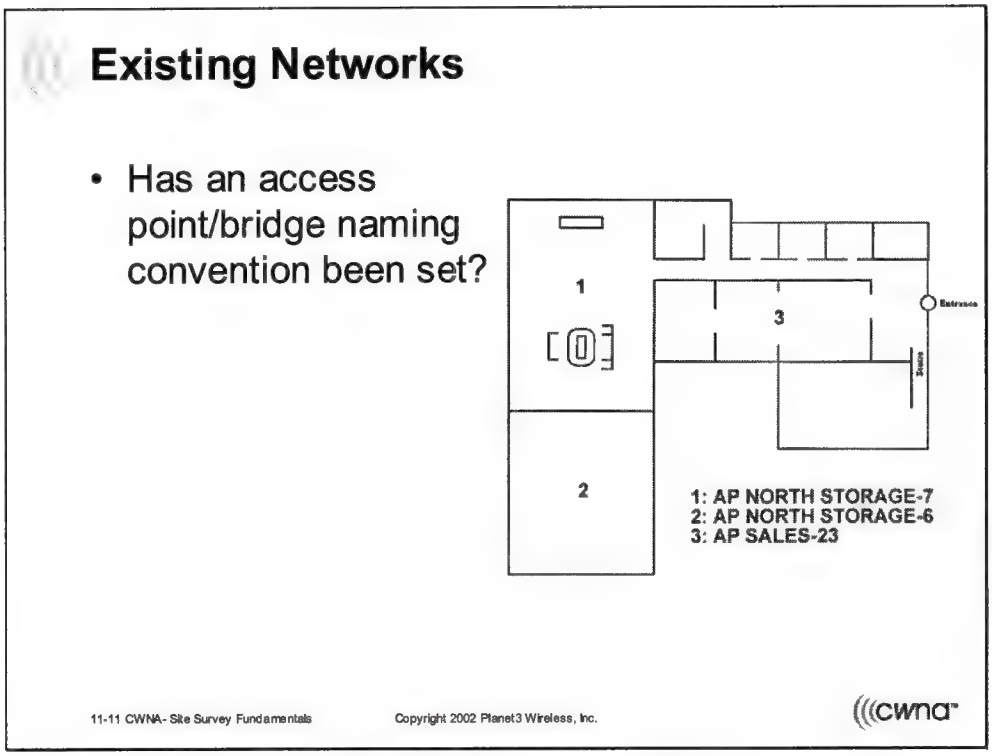
Is a wireless LAN already in place? If so, is it functioning properly?

Documentation of existing wireless LAN hardware, frequencies being used, number of users, throughput, etc., must be taken into account so that decisions can be made on how the new equipment (if needed) will fit in. It may also be the case that the customer did the initial installation, and has since outgrown the initial installation. If the existing setup functions poorly, this poor performance must also be noted so the problems are not repeated.

Often, companies will do a poor site survey that uses far too many access points. Of course, this is a great way for a company to sell access points for a profit, but it doesn't do the customer any favors. Many times a site surveyor will begin the site survey (or re-site survey) by seeing 2-3 times as many access points as are needed. This over coverage can be disastrous for the site surveyor if use of these access points is mission-critical and little to no down-time is allowed due to a production environment.

At any given point in the network, a site surveyor may see possibly as many as 3 access points, with one access point's signal being significantly stronger than the other two. There should be no channel overlap between access points; however, many times this is not the case.

Copyright © 2003, Planet3 Wireless, Inc.

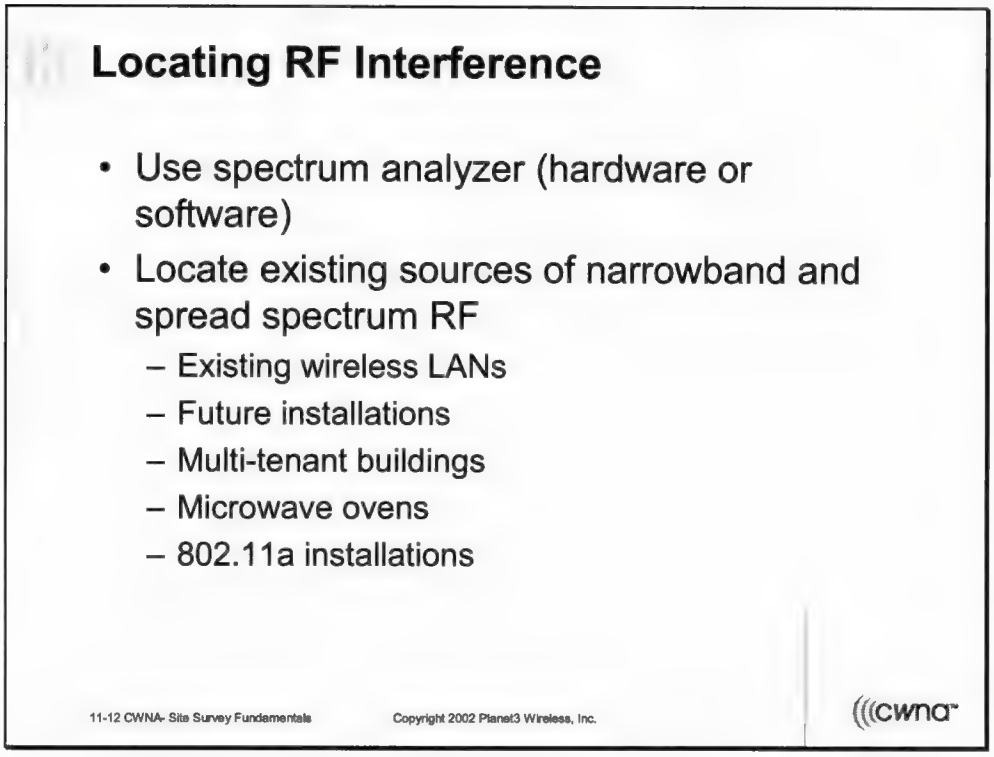


Has an access point/bridge naming convention been devised?

If a wireless LAN is not currently in place, a logical naming convention may need to be devised by the network manager. Using logical naming convention with access points and bridges on the wireless network will make managing them, once they are in place, much easier.

For the site surveyor, having logical names in place for each access point and bridge will facilitate the task of documenting the placement of units in the RF Site Survey Report.

Labeling the cables and patch panels in the wiring closets with the appropriate access point name will make installation and troubleshooting much easier. It will also make any additional site surveying more straightforward.


Locating RF Interference
• Use spectrum analyzer (hardware or software)
• Locate existing sources of narrowband and spread spectrum RF
– Existing wireless LANs
– Future installations
– Multi-tenant buildings
– Microwave ovens
– 802.11a installations
11-12 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Locating RF Interference

Spectrum Analyzer

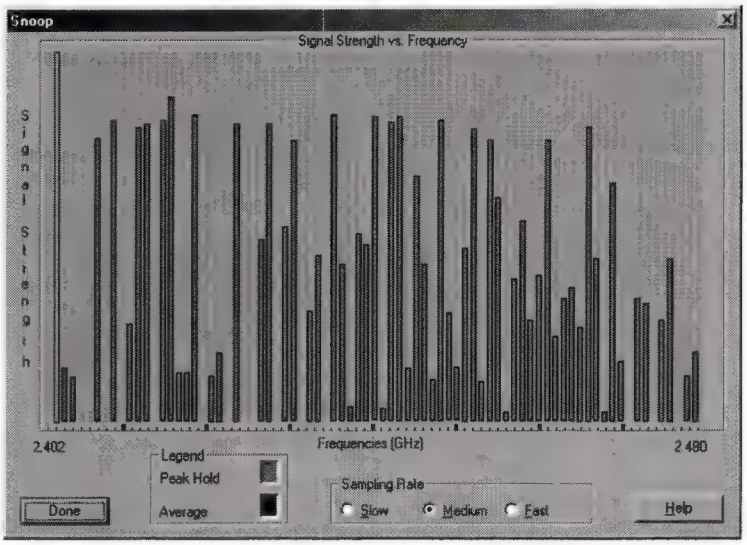
Spectrum Analyzers come in various flavors. The two main categories might be considered software and hardware spectrum analyzers. Hardware spectrum analyzers are made by many manufacturers and may cost many thousands of dollars depending on resolution, speed, frequency range, and many other parameters.

Companies such as Hewlett Packard, Tektronix, Anritsu, and many others make hardware spectrum analyzers. There are companies in the wireless LAN industry who have created software capable of snooping the entire 2.4 GHz range and providing a graphical display of the results. These products give a user the effective equivalent of a hardware spectrum analyzer, which, although it may not produce precisely accurate quantitative measurements, can give a user a general idea of what sources of RF are in use in the area.

Copyright © 2003, Planet3 Wireless, Inc.

Spectrum Analysis

Spectrum Analyzer displaying All-Band Interference

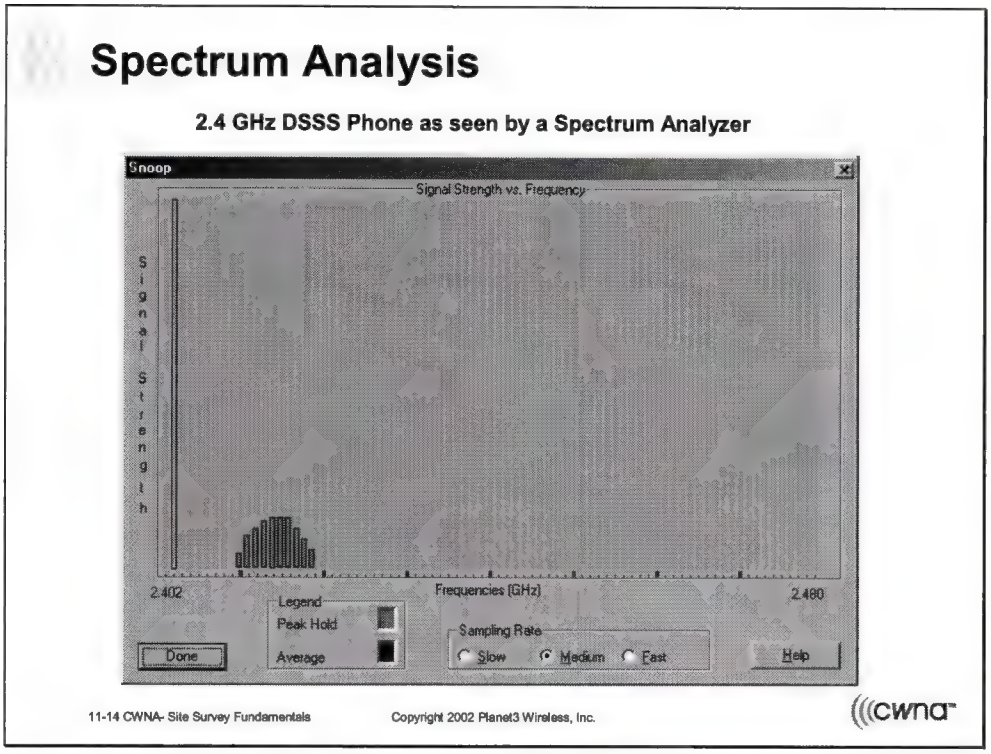


11-13 CWNA- Site Survey Fundamentals Copyright 2002 Planet3 Wireless, Inc. CWNA

As part of the spectral analysis, have all the users turn their equipment off, if possible, so that any sources of background interference can be detected, such as low power sources of narrowband interference. Low power narrowband interference is easily located while there are no other sources of RF in use, but is quite difficult to locate while many sources of RF such as spread spectrum are in use. High power narrowband is easily located with the proper test equipment regardless of additional RF sources.

Part of a spectrum analysis should be to locate any 802.11b or 802.11a networks in use in the area around the implementation area of the proposed wireless LAN. It would be advantageous to both the site surveyor and the customer to know of any 5 GHz RF sources (especially if they are part of a wireless LAN) if current or future plans involve installation of 802.11a products.

After spectrum analysis is complete, an analyzer can be used to find other wireless LANs that are present in the area (perhaps on another floor of a building), which can affect the wireless LAN implementation. The analyzer will pick up any packets being transmitted by a nearby wireless LAN.



Locating Sources of RF

In this phase of the site survey process, questions are asked about potential sources of narrowband and spread spectrum RF interference.

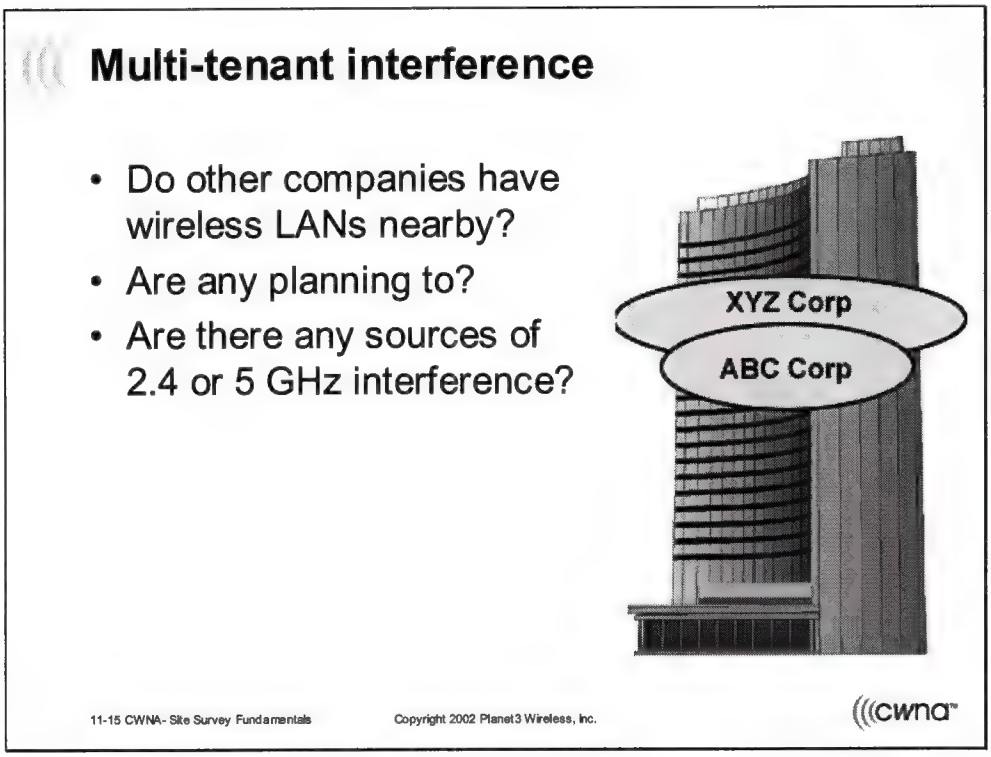
Are there any existing wireless LANs in use in or near the facility?

Existing wireless LANs can cause hardship on a site-surveyor if permission is not provided to disable existing radios. Disabling existing wireless LAN gear may not be possible due to production environments, or the surveyor may have to conduct the site survey during non-production hours.

Are there any plans for future wireless LAN installations other than the one in question?

Determine if there is another wireless LAN project that needs to be included in the analysis. These projects could affect implementation of the wireless LAN for which this site survey is being performed.

Copyright © 2003, Planet3 Wireless, Inc.


Multi-tenant interference
• Do other companies have wireless LANs nearby?
• Are any planning to?
• Are there any sources of 2.4 or 5 GHz interference?
XYZ Corp
ABC Corp
11-15 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

If this is a multi-tenant building, are there any other organizations within the building that have wireless LANs or sources of RF? Are any other organizations planning wireless LAN implementations?

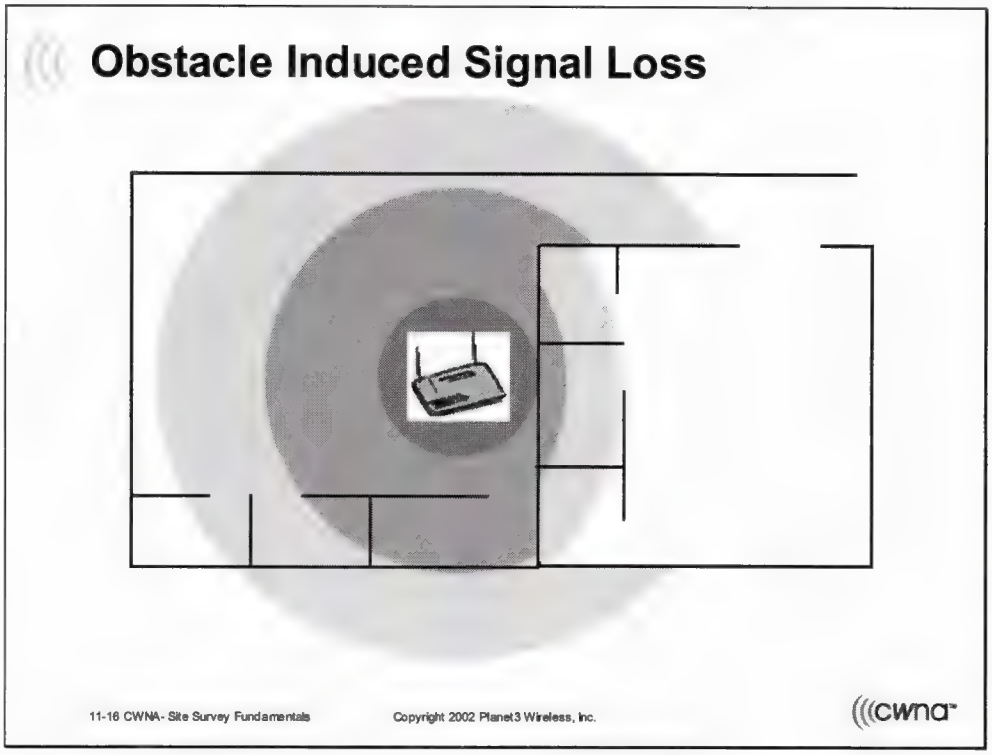
For multi-tenant buildings, it is possible that another organization within the same building is also planning to build a wireless LAN in the future that would impact the site survey. Organizations within the same multi-tenant office building could have wireless LANs in place disrupting each other's communications. If the location is a high-rise building, try to find out if any of the neighboring high-rises have wireless LANs.

Are there any other common sources of RF interference in the 2.4 GHz band in use in the facility?

Microwave ovens, 2.4 GHz cordless phones, radiology equipment, and baby monitors are common sources of RF interference in the 2.4 GHz band. These potential interference sources need to be documented in the survey as potential problems with the installation. Microwave ovens can easily be replaced, though radiology equipment in a hospital installation may not be.

Are there any RF sources in the 5 GHz range (in case 802.11a networks are to be installed)?

If there were many other organizations in the area already using 802.11b, using 802.11a would avoid the interference of trying to coexist with another 802.11b network. However it must also be noted if other 802.11a networks exist in the area that could interfere with an 802.11a implementation.

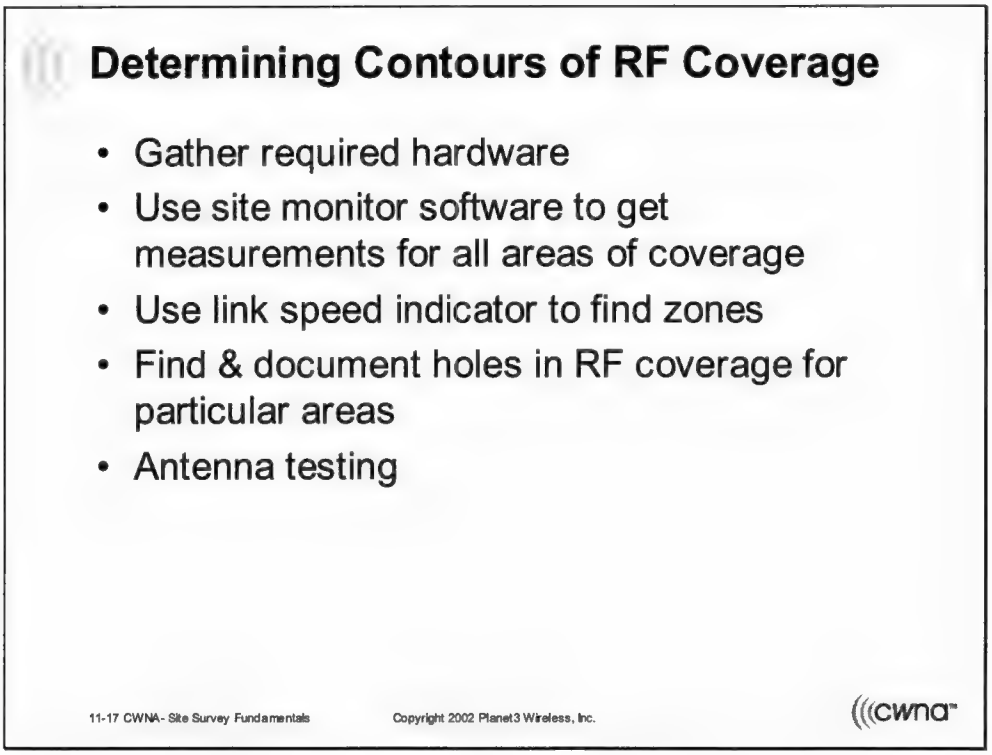


Obstacle-Induced Signal Loss

The following chart provides estimates on RF signal losses that are incurred for various objects. Using these values as a reference will save the surveyor from having to calculate these values. For example, if a signal must penetrate drywall, the range of the signal would be reduced by 50%. The loss is indicated in decibels, and the resulting range effect is shown.

Obstruction	Additional Loss (dB)	Effective Range
Open Space	0	100%
Window (non-metallic tint)	3	70
Window (metallic tint)	5-8	50
Light wall (dry wall)	5-8	50
Medium wall (wood)	10	30
Heavy wall (6" solid core)	15-20	15
Very heavy wall (12" solid core)	20-25	10
Floor/ceiling (solid core)	15-20	15
Floor/ceiling (heavy solid core)	20-25	10

Copyright © 2003, Planet3 Wireless, Inc.


Determining Contours of RF Coverage
• Gather required hardware
• Use site monitor software to get measurements for all areas of coverage
• Use link speed indicator to find zones
• Find & document holes in RF coverage for particular areas
• Antenna testing
11-17 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Determining Contours of RF Coverage

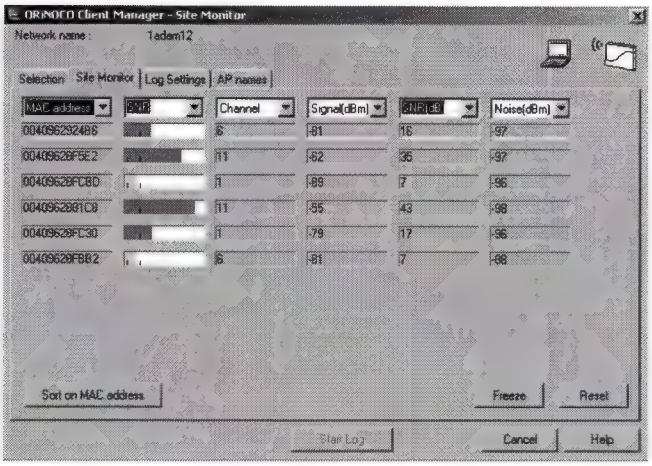
Gathering Needed Hardware

Access points need to be tested in the locations where they might be installed. The coverage is then tested to see if any holes exist in the coverage area. These locations will be marked on the blueprints to be included in the site survey report. The items necessary for determining proper RF coverage are listed below.

- Mobile, battery-powered access point
- Assortment of antennas & double-sided tape
- Small laptop or PDA with extra batteries & a digital camera
- Wireless LAN card, drivers, and site survey software
- Mobile cart to carry ladders & equipment
- Two-way radios & binoculars
- Inclement weather protection (rain suit, umbrella, etc.)
- Blueprints and/or network diagrams
- Pen, paper, & hi-liter
- Toolkit for temporary mounting of hardware

Site Monitor Output

Site Monitor displaying important measurements for multiple access points



11-18 CWNA- Site Survey Fundamentals Copyright 2002 Planet3 Wireless, Inc. ((cwna

Obtaining Measurements

Use site monitor software to obtain the following measurements for all areas of coverage:

- Signal Strength (dBm)
- Signal-to-Noise Ratio (dB)
- Noise Strength (dBm)

To verify a good connection to a particular access point, a link test utility can be used. A link test utility gives more specific information about the wireless connection between the access point and the wireless station.

Locating Zones

Use a link speed indicator (part of the manufacturer's utility software) to find zones for 1, 2, 5.5, & 11 Mbps coverage areas around the access point. This piece of documentation is important for meeting throughput requirements of users of varying distances from the access point.

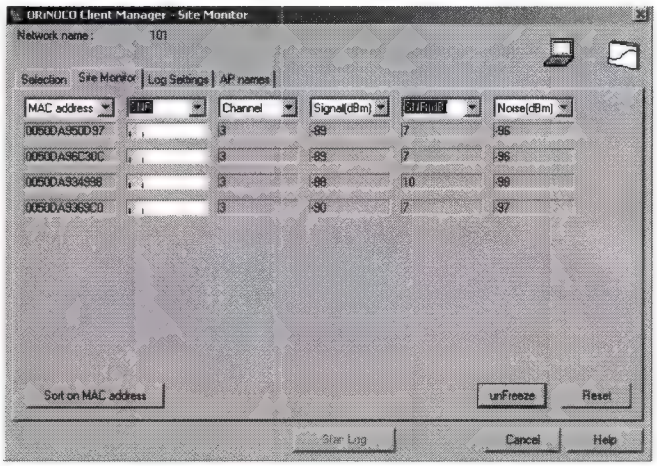
Documenting Coverage Gaps

Gaps (or "holes") in RF coverage for particular areas need to be located and documented. Documenting gaps in coverage will generally be in two forms - written text and illustrations.

Copyright © 2003, Planet3 Wireless, Inc.

Site Monitor Output

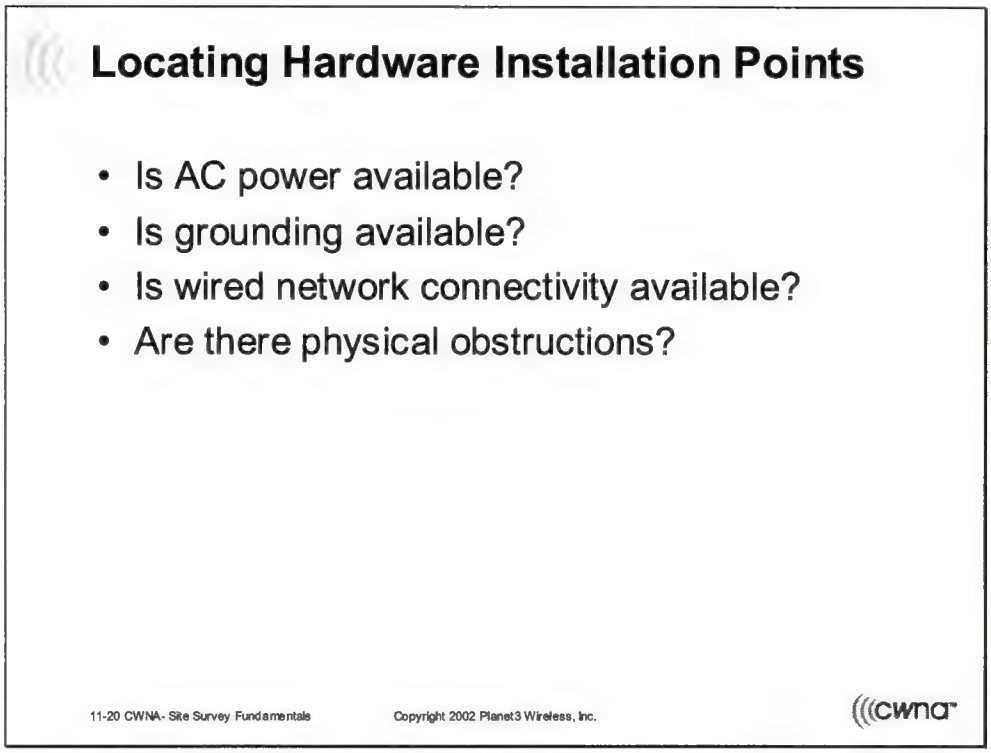
Site Monitor displaying important measurements for multiple access points



11-19 CWNA- Site Survey Fundamentals Copyright 2002 Planet3 Wireless, Inc. ((cwna

Antenna Testing

Various types of antennas can be used for site survey testing including highly directional, semi-directional, and omni-directional. When using semi-directional antennas, be sure to take into account the side and back lobes both for coverage and security reasons. Sites may require the use of multiple antenna types to get the appropriate coverage. Long hallways might benefit from Yagi, patch, or panel antennas while omni-directional antennas would more easily cover large rooms.


Locating Hardware Installation Points
• Is AC power available?
• Is grounding available?
• Is wired network connectivity available?
• Are there physical obstructions?
11-20 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Locating Hardware Installation Points

Some questions to consider when looking for the best place to install wireless LAN hardware follow.

Is AC power available?

Without an available source of AC power, access points will not function. If AC power is not available in a particular location, an electrician's services may be required (added cost) or Power over Ethernet (PoE) can be used to power the unit.

Is grounding available?

Proper grounding for all wireless LAN equipment will provide added protection against stray currents from lightning strikes or electrical surges.

Is wired network connectivity available?

If network connectivity is not available, an access point will need to be operated in repeater mode to provide network connectivity. Using access points as repeaters is not a desirable scenario, and the network performance would be much better if the access point could be wired to the network.

If the distance between the access point and the network connection is more than 100 meters, an access point can be used that supports a fiber connection.

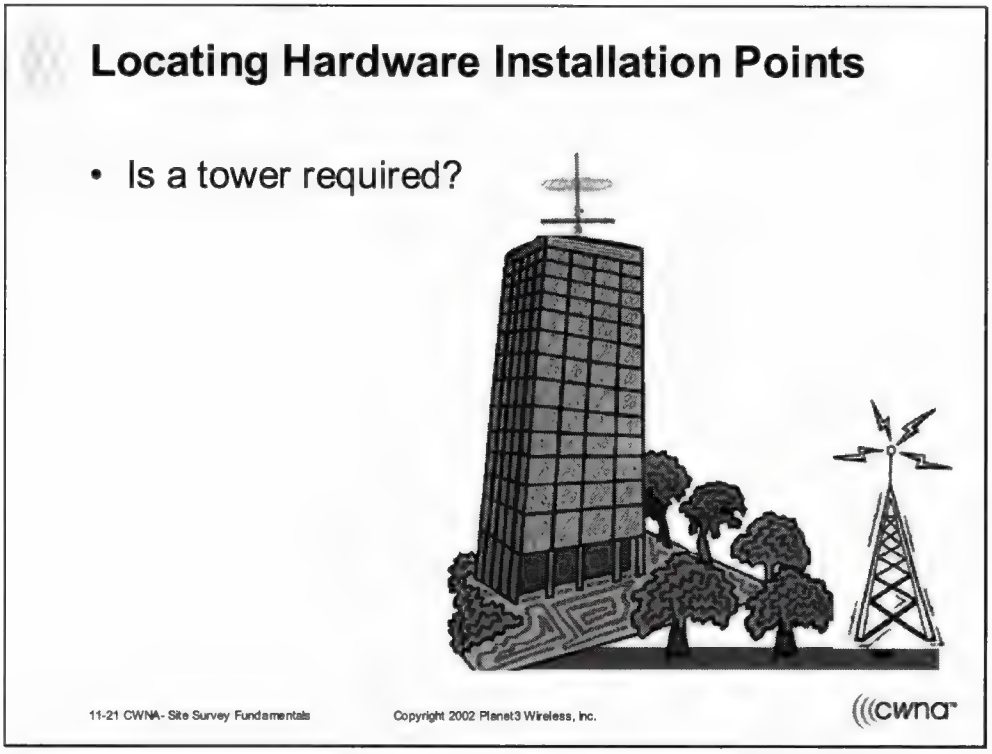
Copyright © 2003, Planet3 Wireless, Inc.

However, using an access point that has fiber network connectivity negates the use of PoE and would require a source of AC power nearby.

Are there physical obstructions?

Doorways, cement ceilings, walls, or other obstructions can result in some type of construction costs if they need to be altered to allow for power connections or to run power or data cabling to the access points or antennas.

Copyright © 2003, Planet3 Wireless, Inc.


Locating Hardware Installation Points
• Is a tower required?
11-21 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Towers

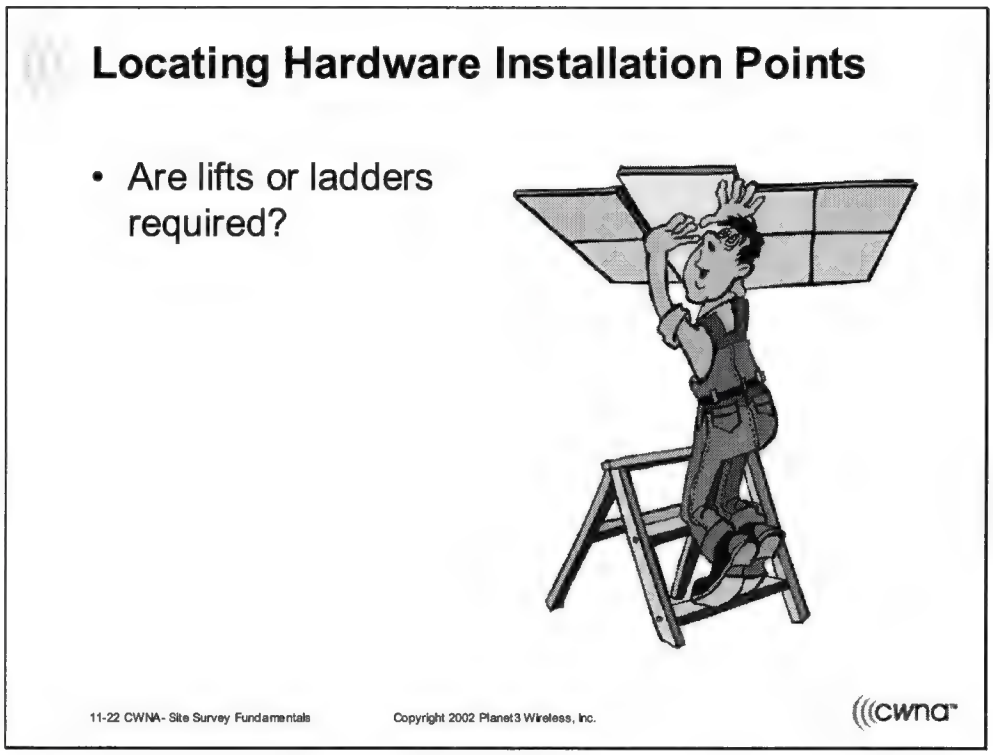
Is a tower required?

When performing a site survey, it may be discovered that a 30-foot tower is needed on top of a building to clear some trees that are in the direct signal path of an outdoor wireless link. If a tower is required, other questions that need to be asked might include:

If the roof is to be used, is it adequate to support a tower?
Is a structural engineer required?
Is a permit necessary?

A structural engineer may be required to determine if a tower can be placed on top of a building without safety risks to the inhabitants of the building. Permits or government approval may also be necessary to install a tower. For example, for towers that are more than 200 feet above ground level, the FCC requires that the FAA be notified prior to constructing or modifying an antenna structure (tower, pole, building, etc.). A 190-foot tall building with an 11-foot tall tower would fall into this category for example because the building (antenna structure) has been modified and exceeds 200 feet. Local municipalities must approve the building of any type of structure (antenna structures or otherwise), thus the installer/designer of such a structure should obtain proper permissions or licenses.

Copyright © 2003, Planet3 Wireless, Inc.


Locating Hardware Installation Points
• Are lifts or ladders required?
11-22 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Lifts and Ladders

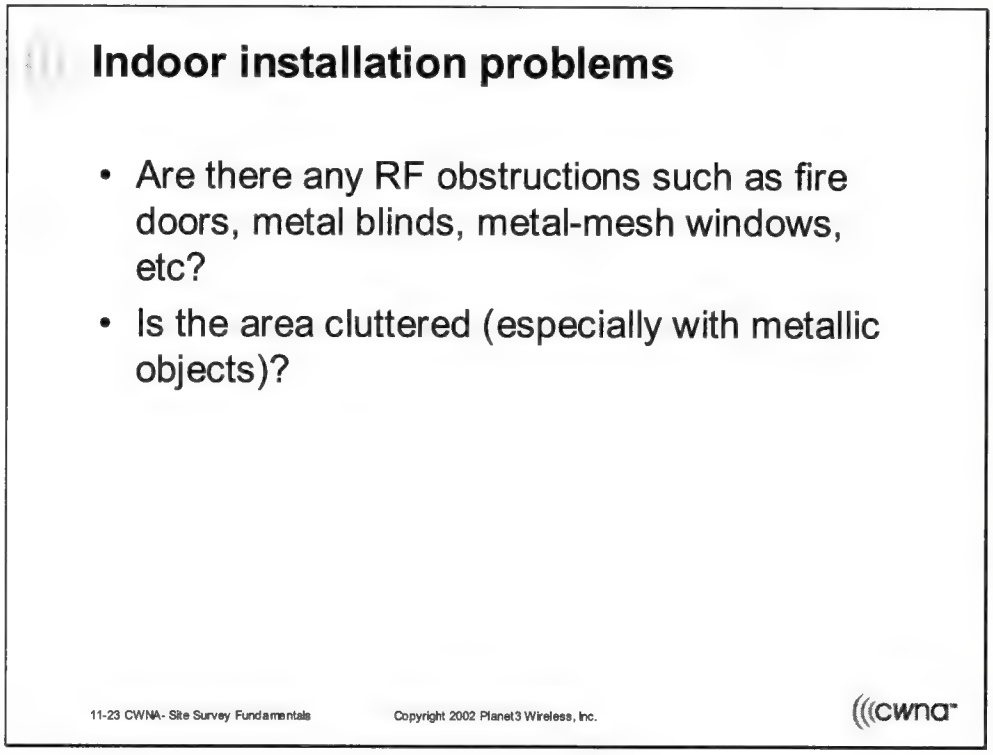
Are lifts or ladders required?

Lifts and ladders could be needed for an area where a trade show or other similar function is going to take place. The event's location may have 40' ceilings and the access points may need to be mounted in the ceiling for proper coverage.

OSHA has many regulations regarding ladders and ladder safety. If a facility such as a trade show is able to provide the personnel, ladders, and lifts to do the installation, it is recommended to let these individuals perform the work. These individuals are familiar with OSHA regulations and have processes in place to obtain the proper permits.

The RF Site Survey Report will need to reference any lifts, ladders, or permits required for installation of the wireless LAN.

Documenting Installation Issues


Indoor installation problems
• Are there any RF obstructions such as fire doors, metal blinds, metal-mesh windows, etc?
• Is the area cluttered (especially with metallic objects)?
11-23 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Indoor Installation Issues

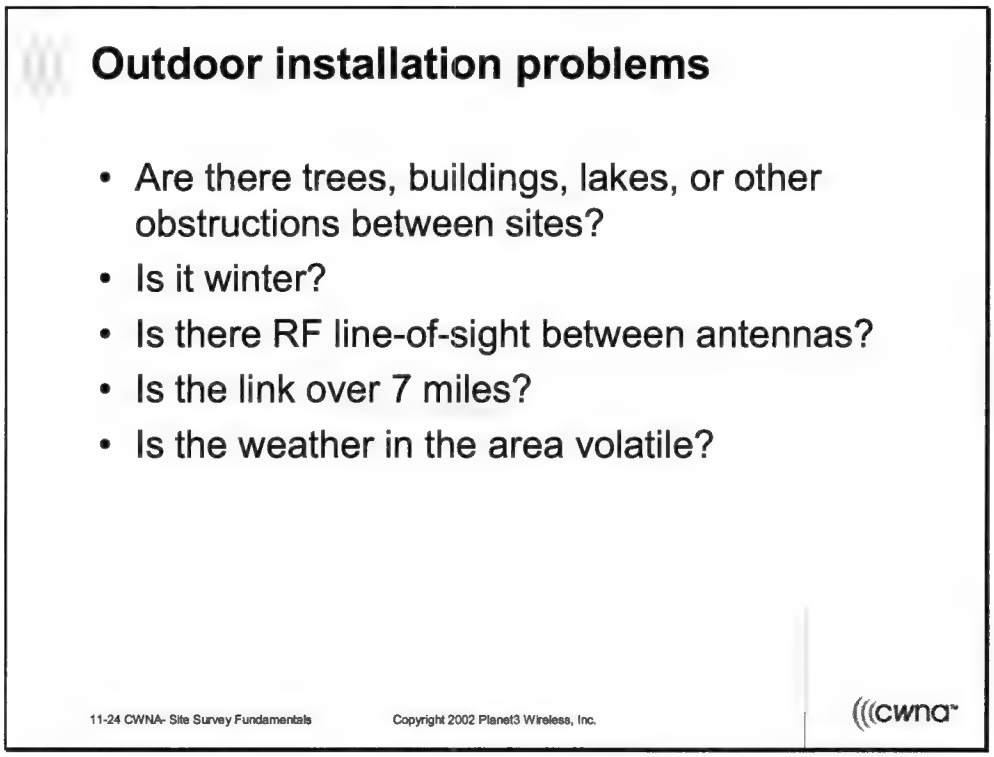
Are there any RF obstructions such as fire doors, metal blinds, metal-mesh windows, etc?

Obstructions may not be as much of an issue if the signal does not need to go through objects. However, some objects can cause multipath. Rooms that are filled with metal blinds need to be tested with all of the blinds down (worst case) and all of the blinds up (best case) to determine the impact on the RF signals.

Is the area cluttered (especially with metallic objects)?

A large open space with a cube farm is considered a cluttered environment. This area would contain a number of computers, filing cabinets, short walls at different angles, and the cubes themselves, which are usually metal structures.

Copyright © 2003, Planet3 Wireless, Inc.


Outdoor installation problems
• Are there trees, buildings, lakes, or other obstructions between sites?
• Is it winter?
• Is there RF line-of-sight between antennas?
• Is the link over 7 miles?
• Is the weather in the area volatile?
11-24 CWNA- Site Survey Fundamentals
Copyright 2002 Planet3 Wireless, Inc.
cwna

Outdoor Installation Issues

Are there trees, buildings, lakes, or other obstructions between sites?

Any outdoor obstruction must be noted in the report as a potential point of interference if it lies in the direct signal path of the outdoor link.

Is it winter?

In the winter, seasonal trees may not have any leaves on them. These trees may not cause any problems by intruding into the Fresnel Zone at present, but in the springtime, when trees begin to blossom and hold more water, the RF signal could be impacted. Trees that bloom in the spring should be recorded as part of the report. Pine trees are less of a problem in this regard then other broad leaf trees.

Is there RF line-of-site between antennas?

In the winter time there could be visual and RF LOS, but once the trees have leaves on them, the Fresnel zone may be compromised and RF LOS may no longer exist.

Is the link over 7 miles?

When a wireless link is over 7 miles long, Earth bulge will be a factor. Earth bulge, or the curvature of the Earth, will affect RF LOS. Visual LOS can be available over 7 miles in places like desert areas, but the earth bulge will intrude upon the Fresnel Zone, interfering with the RF signal.

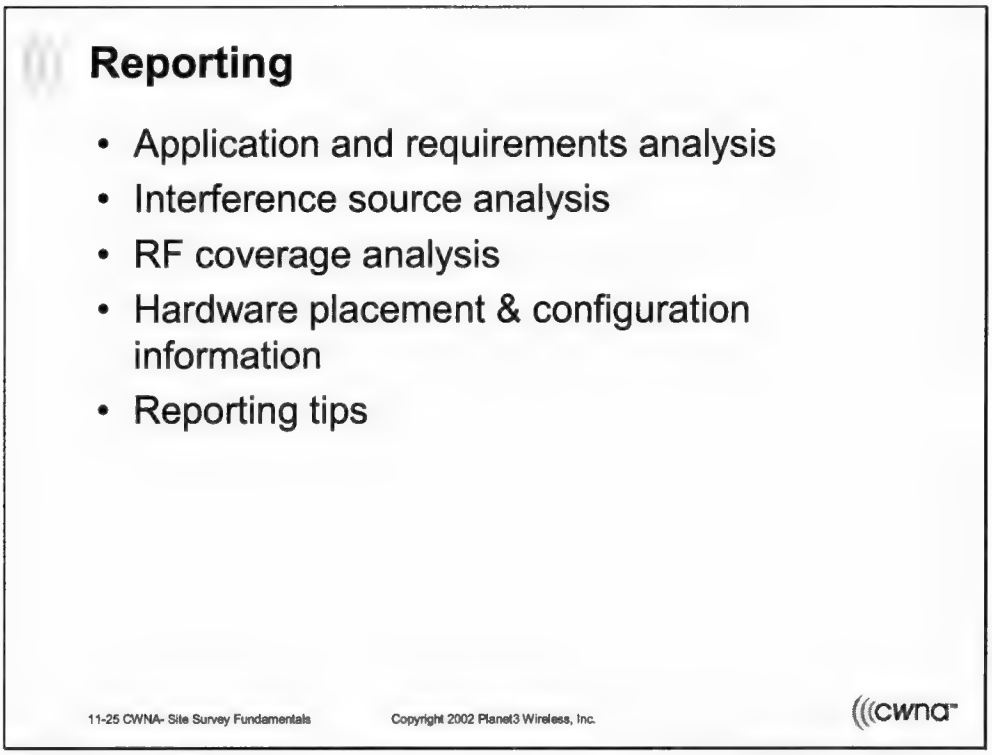
Is the weather in the area volatile?

When a parabolic dish antenna is mounted on top of a limber pole outside, the wind will move it around and displace the RF signal. Be aware that the wind may not be blowing on the day the site survey is done, but it can become a factor at a later time or during a different season. If wind is a problem, consider using a grid antenna, which are perforated to allow air to pass through.

Consider whether or not lightning rods may be needed if the area is known for excessive lightning. The cost of lightning rods and their installation is expensive but can save money compared to excessive network downtime if they are not used.

Rain does not cause a significant amount of degradation in an RF wave front, but water can seep into cabling or connections when they are not sealed properly, wreaking havoc with the RF hardware.

Copyright © 2003, Planet3 Wireless, Inc.



Reporting

In the early stages of the process, the network manager was interviewed to find out what the design goals and user requirements were for the wireless LAN. The RF site survey report includes an item-by-item listing of what these requirements were, and how the site survey addressed each one. For example, a report might say that there are 100 users in this particular room each day at 2pm in need of wireless LAN services. It will also address the facts that three access points will be needed and they will have to be placed in the center of the room at the ceiling in order to provide adequate coverage.

Application and requirements analysis

The report should answer the following about customer application requirements:

What applications will be used over the wireless LAN and what are their requirements?
What are the requirements of the wireless LAN in general? Is there a QoS expected?
Where and how is the wireless LAN to be used? Is seamless roaming a requirement?

Interference source analysis

RF interference and obstruction findings will indicate locations of RF interference sources. Sources of RF Interference that will not affect the wireless LAN implementation can be ignored unless they will affect future installations, in which case they should be documented in the report.

The report should answer the following about RF interference sources:

What are the sources of RF interference?
Where are the sources of RF interference?
Can the RF interference sources be removed?
Will the RF interference source affect the wireless LAN?

RF coverage analysis

The report should answer the following questions regarding RF coverage:

What areas have what coverage levels?
What overlapping coverage is provided?
Are there any gaps in coverage?

Hardware placement & configuration information

The report should answer the following questions about hardware placement and configuration:

What is the name of each manageable device?
Where and how should each access point and bridge be placed or mounted for maximum effectiveness?
What channels should each access point be on?
How much output power should each access point deliver?

A list of facts about each access point to be installed (or already installed) should be included in the RF site survey report. This list should include (as a minimum):

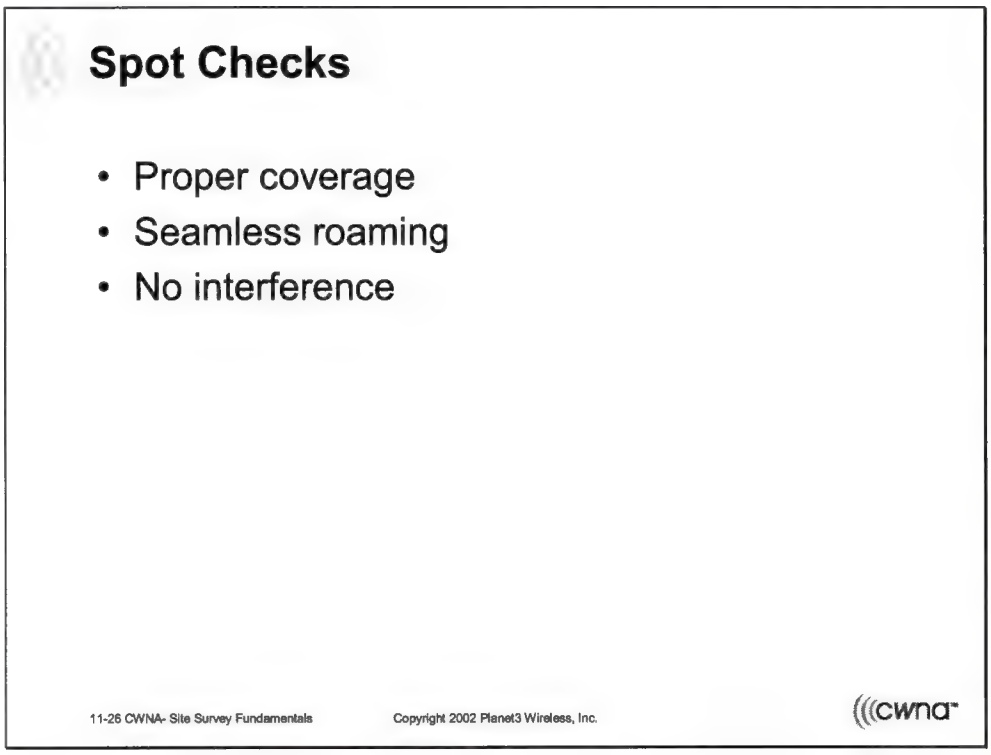
- Name of device
- Location within facility
- Antenna type to be used
- Power output settings
- Connectors & cables to be used
- Antenna mount type to be used
- How power should be provided to unit
- How data should be provided to unit
- Picture of location where unit is to be installed

Copyright © 2003, Planet3 Wireless, Inc.

Reporting tips

Customers will require drawings so they can see how everything is going to be configured and how the configuration may impact the existing infrastructure of the network and the facility. Provide screenshots of the site monitor software & digital pictures outlining locations of access points and bridges. Also provide Visio, CAD drawings, or marked-up blueprints to help illustrate the findings and suggestions.

Copyright © 2003, Planet3 Wireless, Inc.

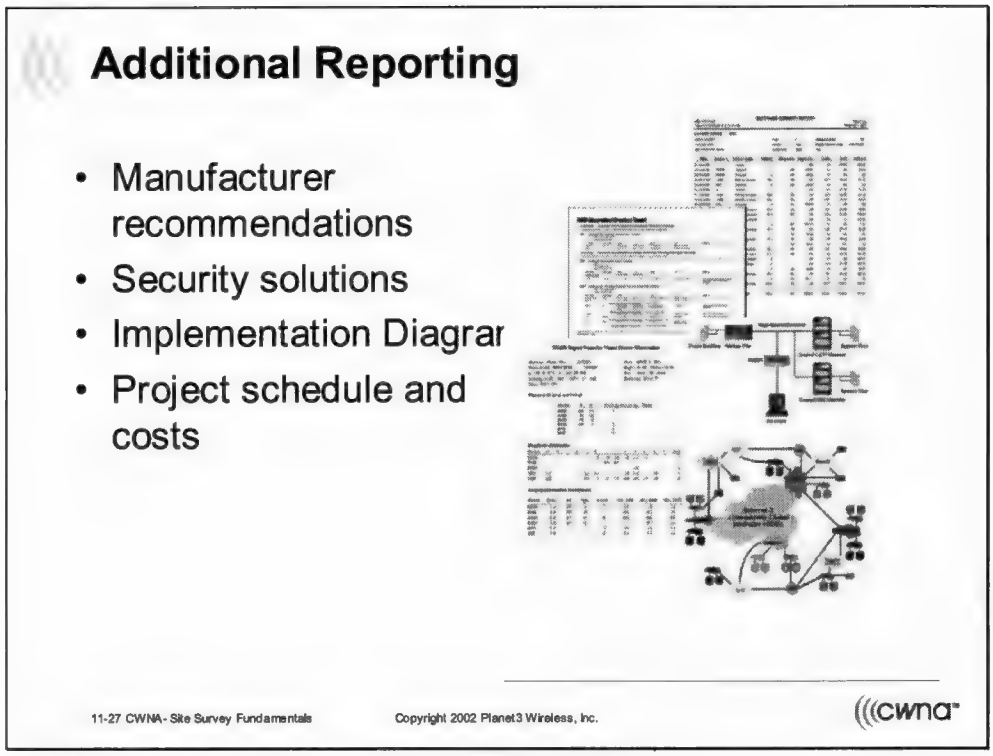


Spot Checks

After a wireless LAN is installed, it might not work exactly as planned, although it may be close. Spot-checking, done by a site surveyor after installation is complete, is most helpful in avoiding troubleshooting situations during production use of the network. Items that should be checked are:

- Coverage in perimeter areas
- Overlapping coverage for seamless roaming
- Co-channel and adjacent channel interference in all areas

Copyright © 2003, Planet3 Wireless, Inc.



Additional Reporting

The RF site survey's purpose is to document coverage, hardware placement, and RF interference sources.

There are other reports that can be included along with the site survey report. Consultants may charge additional money for a report that includes information about one or more of the following:

- Which manufacturers make appropriate products for this environment and what those particular products are
- Which security solution makes sense for this environment and how to implement it
- Detailed diagrams and drawings on how to implement solutions
- Cost and time involved to implement solutions
- Details of how each wireless LAN requirement listed in the RF site survey was met (item-by-item)

It is typically desirable to do as much business with a company as they will allow (provided the business is profitable), so working with the project manager or sales professional is suggested when there is considerable wireless LAN work to be done. Not handling this situation effectively can sometimes lead to the customer's trying to perform the installation or hiring another company to implement the solution recommended from the site survey.

Recommendations for equipment vendors are very important, and require:

- Knowing what each vendor specialized in, their strengths, and weaknesses
- What level of support is available from a vendor and how easy it is to get replacement hardware
- What market space each vendor is in
- The costs of the appropriate hardware

When a customer reads the consulting report, they may determine that another vendor offers better or cheaper hardware that can provide the same functionality. Part of the recommendation is to include justification for the decision in choosing a particular vendor's hardware. A bill of materials can be included outlining each piece of hardware needed and the cost of each item.

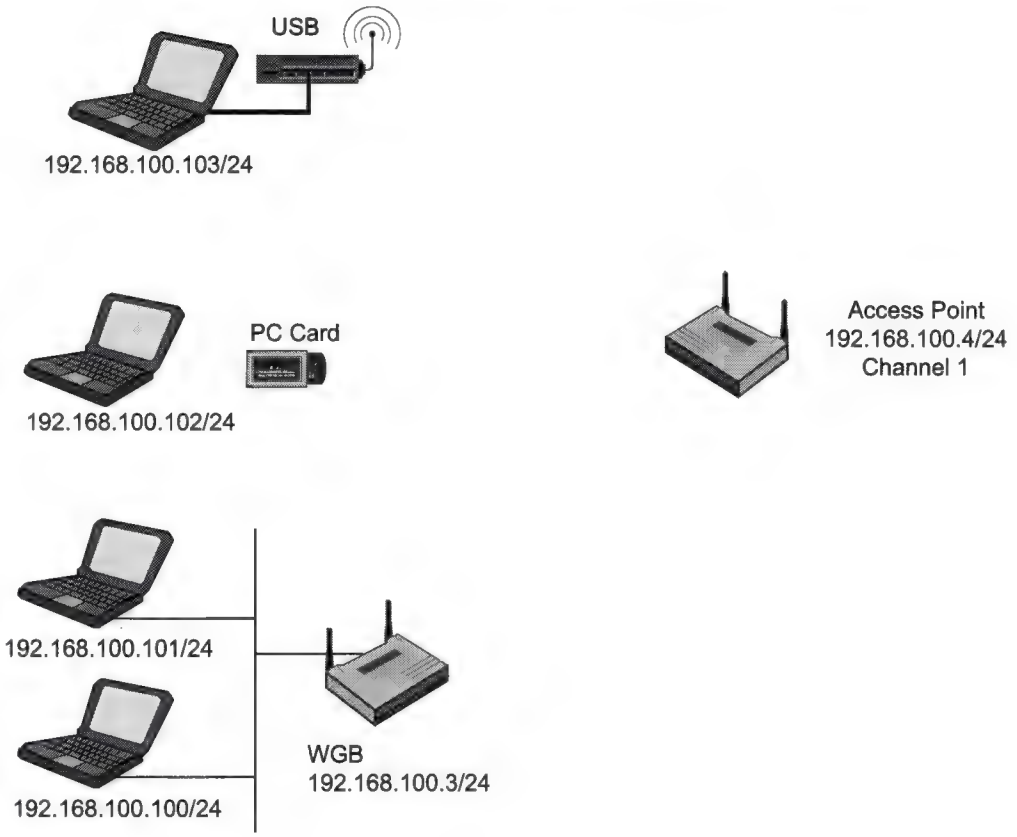
Copyright © 2003, Planet3 Wireless, Inc.

Chapter

12 Lab Exercises

Copyright © 2003, Planet3 Wireless, Inc.

Lab 1: Infrastructure Mode Connectivity



Objectives

After completing this lab, you will be able to demonstrate how a wireless client authenticates and associates to an access point using RF technology.

Hardware/Software Required

- 2 Laptop Computers
- 2 Desktop Computers
- 1 Access Point
- 1 wireless LAN PC Card
- 1 wireless LAN USB Client
- 1 Workgroup Bridge
- 1 Ethernet hub

Copyright © 2003, Planet3 Wireless, Inc.

Summary

Access points maintain a table of actively connected users. This table is called the "association table" or "learning table" and contains information such as the MAC address, IP address, computer name, and status of the associated stations. The status of each client is shown in the association table (depending on the equipment vendor), and each client can be in one of the following states:

- Not authenticated and not associated
- Authenticated but not associated
- Authenticated and associated

The authentication process happens before the association process. To complete the association and authentication processes, certain settings are required at both the access point and the client stations. These settings are as follows:

- The SSID setting on each wireless client must match the SSID setting on the access point
- If WEP is used, WEP keys must match exactly
- WEP must be configured in the same way on both ends of the connection (either off or on)
- Client stations and access points must have enough power output to reach each other with their RF signal
- The access point must support and be set for the same authentication process used by the client station

Process

1. **Configure the network**
    a. Connect the two desktop computers and the workgroup bridge to the hub
    b. Connect the USB client to one laptop computer
    c. Connect the PC Card to one laptop computer
    d. Configure all hosts for a flat IP subnet
2. **Configure the access point**
    a. Channel 1
    b. SSID=101
    c. No WEP
    d. Open System Authentication

Copyright © 2003, Planet3 Wireless, Inc.

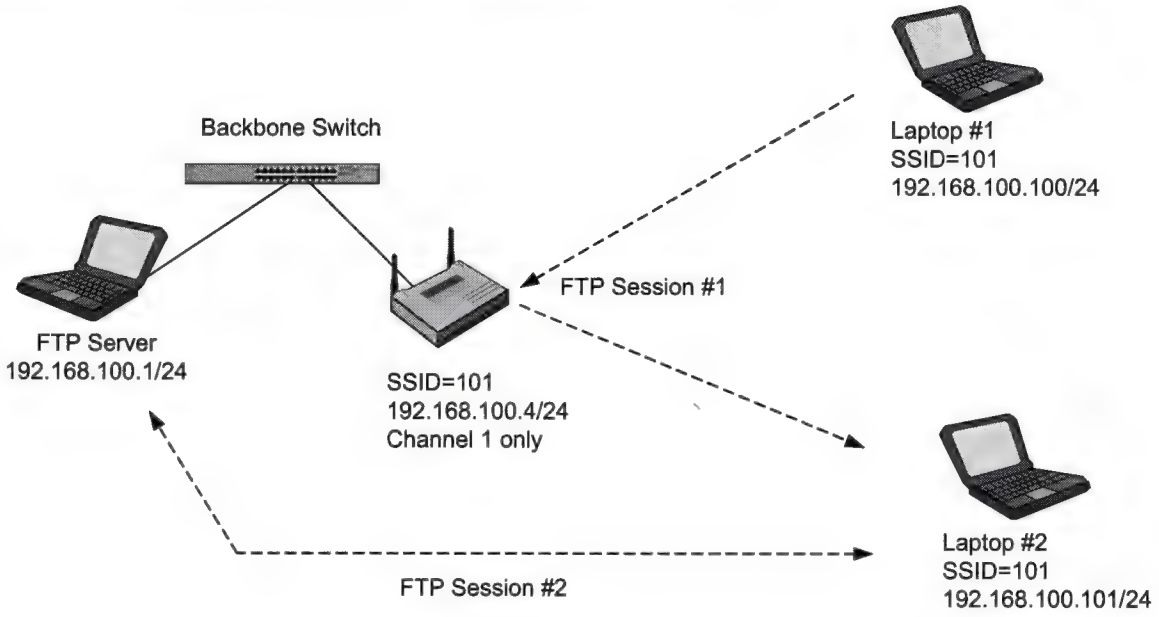
3. **Configure wireless clients**
    a. Install and configure drivers (where required)
    b. Install and configure wireless LAN utility software
    c. SSID=101
    d. No WEP
4. **View the Association Table**
    a. By viewing the access point's association table, clients can be seen authenticating and associating to the access point. The association table is viewed via web browser (http) or console port in most access points.
5. **Test connectivity**
    a. Test connectivity between wireless clients and the access point by pinging the access point and other wireless clients.
6. **Note functionality of Workgroup Bridge**
    a. Verify that the Workgroup Bridge connects the wired clients behind it as a single collective client by viewing its entry in the association table.

Troubleshooting

1. Verify WEP & SSID settings are correct on clients and the access point
2. Verify drivers are properly loaded on the wireless LAN clients
3. Check the association table in the access point to find the status of a particular wireless LAN client
4. Verify clients are configured in "Infrastructure Mode"
5. Verify no MAC filters are configured on the access point
6. Verify radios are turned on in the access point and in the wireless LAN clients

Copyright © 2003, Planet3 Wireless, Inc.

Lab 2: Infrastructure Mode Throughput Analysis



Objectives

In this lab, the half-duplex nature of wireless LANs will be demonstrated. Also shown will be that frames move from wireless client to wireless client across the access point (access point relay).

Hardware/Software Required

- 2 Laptop Computers
- 1 Desktop Computers
- 2 wireless LAN PC Cards
- 1 Access Point
- 1 Hub
- Throughput measuring software
- FTP client software
- FTP server software

Copyright © 2003, Planet3 Wireless, Inc.

Summary

This lab exercise demonstrates that a wireless LAN is a half-duplex networking environment and that frames moving from one wireless client to another wireless client must traverse the access point. These concepts are demonstrated by first moving a file using the FTP protocol between a wireless node and a wired node. During the file transfer, throughput will be monitored using the throughput-measuring software on the FTP client. The actual throughput will typically be around 50% or less of the rated bandwidth of the system in use. For example, in 11Mbps mode, you might expect approximately 5 Mbps of throughput between wireless and wired hosts.

When moving the same file between two wireless clients, notice that the expected throughput is cut in half (or less) - down to approximately 2.5 Mbps. The reason for this decrease is that each frame must be sent to the access point, then the access point must contend for network access in order to forward the frame to the destination wireless client. If the file were moving directly between wireless clients, you would expect to see approximately the same 5 Mbps of throughput seen between wireless and wired hosts. When sending the file between the wireless host and the wired host, the frame must only traverse the wireless LAN once causing no multi-client contention for medium access.

Process

1. **Configure the network**
   a. Install and configure FTP server software on desktop computer
   b. Install and configure FTP server software on laptop computer #2
   c. Install and configure FTP client software on laptop computer #1
   d. Install and configure throughput-measuring software on laptop computer #1
   e. Configure all hosts for a flat IP subnet
2. **Configure the Access Point**
   a. Channel 1
   b. SSID=101
   c. No WEP
   d. Open System Authentication
3. **Configure wireless clients**
   a. Install and configure drivers (where required)
   b. Install and configure wireless LAN utility software
   c. SSID=101
   d. No WEP

Copyright © 2003, Planet3 Wireless, Inc.

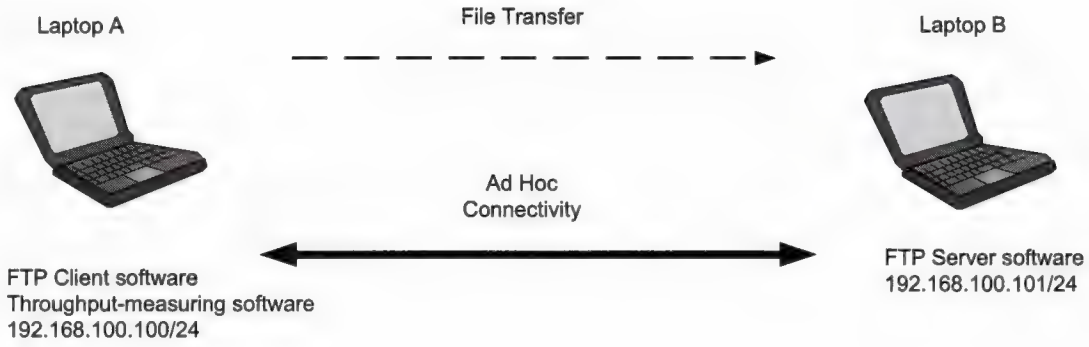
4. **First file transfer**
    a. Start file transfer from Laptop #1 to desktop computer
    b. Record average throughput
5. **Second file transfer**
    a. Start file transfer from Laptop #1 to Laptop #2
    b. Record average throughput
6. **Analyze differences between file transfers**
    a. Note the wireless-to-wireless transfer has approximately half of the throughput of the wireless-to-wired transfer

Troubleshooting

1. Verify WEP & SSID settings are correct
2. Verify drivers are properly loaded on the wireless LAN clients (where required)
3. Check association table in access point to find status of a particular wireless LAN client
4. Verify clients are configured in "Infrastructure Mode"
5. Verify no MAC filters are configured on the Access Point
6. Verify radios are turned on in the access point and in the wireless LAN clients
7. Verify username and password on each FTP server are correctly matched with the FTP client
8. Verify connectivity between all devices using PING

Copyright © 2003, Planet3 Wireless, Inc.

Lab 3: Ad Hoc Connectivity & Throughput Analysis



Objective

In this lab, wireless LAN clients will connect to each other without an access point. Throughput will be calculated, and it will be demonstrated that manufacturer's hardware and drivers can often make a difference in the throughput of a system.

Hardware/Software Required

- 2 wireless LAN PC Cards (vendor A)
- 2 wireless LAN PC Cards (vendor B)
- 2 laptop computers
- FTP Server software
- FTP Client software
- Throughput measuring software

Copyright © 2003, Planet3 Wireless, Inc.

Summary

An Ad Hoc network is configured using two or more wireless LAN clients and no access point. The clients must be configured on the same channel using the same SSID. The WEP, authentication, and mode settings must also match for each client for them to associate (connect) with one another. The reason for defining the channel on the clients is that there is no access point broadcasting beacons, which notify clients of channel information. Some vendors offer multiple Ad Hoc modes (both standard and proprietary) and some may be incompatible with others. For this reason, this lab will use PC cards from like vendors for each test. Some operating systems may not allow the channel to be configured in Ad Hoc mode. In this case, a different operating system that allows channel configuration in ad hoc mode must be used in conjunction with the one that does not.

Once both clients are fully configured with "vendor A" PC cards, check basic connectivity with the PING utility on either side of the connection. Transfer a file using the FTP protocol between the laptop computers. During the file transfer, monitor the throughput measuring software on the FTP client. Record the throughput between wireless LAN clients. It is likely that the throughput is less than the ~5 Mbps typically seen in Infrastructure mode using an access point.

Reconfigure clients with "vendor B" PC cards and follow each test a second time. This time, it is likely that your throughput has varied enough to notice depending on the PC card manufacturers chosen.

Process

1. **Configure the network**
   a. Install and configure FTP server software on laptop computer #2
   b. Install and configure FTP client software on laptop computer #1
   c. Install and configure throughput-measuring software on laptop computer #1
   d. Configure both hosts for a flat IP subnet
2. **Configure wireless clients (vendor A)**
   a. Install and configure drivers for "vendor A" PC cards
   b. Install and configure wireless LAN utility software
   c. No WEP
   d. Ad Hoc Mode (also called Peer-to-Peer mode)
   e. Channel 1
   f. SSID=101
3. **File transfer**
   a. Start file transfer from Laptop #1 to Laptop #2
   b. Record average throughput

Copyright © 2003, Planet3 Wireless, Inc.

4. **Analyze file transfer**
   a. Is the throughput lower, higher, or the same as when using an access point?
   b. If the throughput is different, why?
5. **Configure wireless clients (vendor B)**
   a. Install and configure drivers for "vendor B" PC cards
   b. Install and configure wireless LAN utility software
   c. No WEP
   d. Ad Hoc Mode (also called Peer-to-Peer mode)
   e. Channel 1
   f. SSID=101
6. **File transfer**
   a. Start file transfer from Laptop #1 to Laptop #2
   b. Record average throughput
7. **Analyze File transfer**
   a. Was this file transfer faster or slower than with vendor A?

Troubleshooting

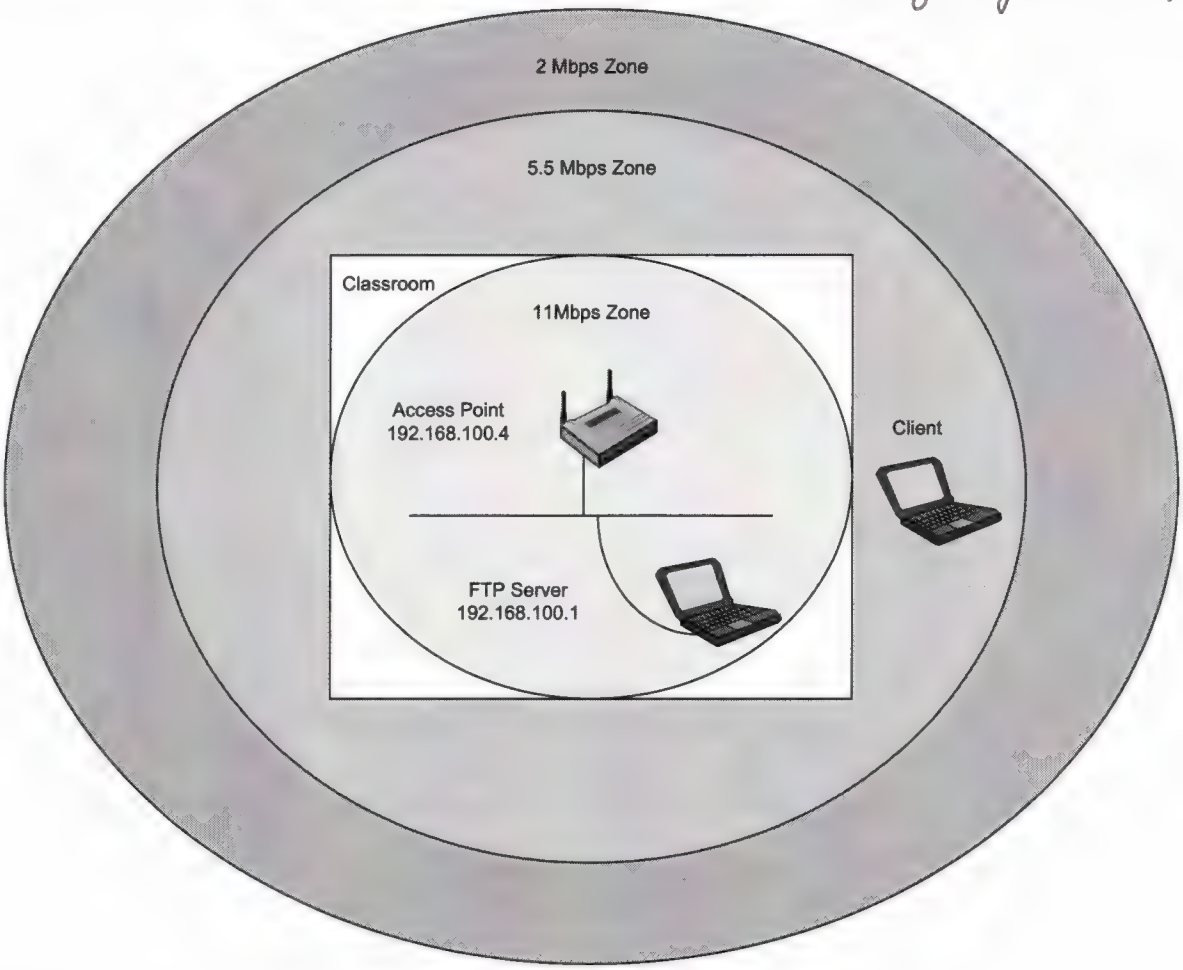
1. Verify WEP & SSID settings are the same on both laptops
2. Verify drivers are properly loaded on the wireless LAN clients
3. Verify clients are configured in "Ad Hoc Mode"
4. Verify radios are turned on in the wireless LAN clients
5. Verify username and password on the FTP server is correctly matched with the FTP client
6. Verify connectivity between devices using PING

Copyright © 2003, Planet3 Wireless, Inc.

00:06:FD:E3:5E:67

Lab 4: Cell-sizing and Automatic Rate Selection (ARS) in Infrastructure Mode

site survey:
how far you can get 1 Mbps



Objective

In this lab exercise, cell sizing and ARS will be demonstrated. Cell sizing is important for seamless connectivity while roaming and for security purposes. ARS is the wireless LAN client's ability to speed up or slow down the wireless connection in order to maintain optimum connectivity with the access point. Additionally, this lab will show the effects that different items in the environment can have on wireless LAN performance.

Hardware/Software required

- 1 Access Point (with variable output power)
- 1 Laptop Computer
- 1 Hub

Copyright © 2003, Planet3 Wireless, Inc.

- 1 Desktop Computer
- 1 wireless LAN PC Card (with variable output power)
- FTP Server software
- FTP client software
- Throughput-measuring software

Summary

This lab exercise will demonstrate how output power affects the sizes of the zones of coverage within the cell. The zones are concentric bands of coverage around the intentional radiator (the access point in this case). These zones are coverage zones at given speeds of connectivity (11, 5.5, 2, 1 Mbps). 802.11b-compliant wireless LAN client devices are designed to adapt to higher or lower rates as dictated by the received signal strength, bit error rate, signal to noise ratio and other information from the access point. The signal strength is based primarily on distance from the access point, but can also be affected by RF noise and interference.

Notice that while walking away from the access point how the client will automatically change (lower) connectivity speed in order to maintain the connection. This functionality is commonly known as Automatic Rate Selection or Dynamic Rate Shifting. Notice also that as output power at the access point is increased, the thickness of the zones increases, even if only slightly. At higher output power settings (30mW, 100mW, etc), the zones become even more defined. Without any significant amount of data being transferred between the wireless client and the FTP server, ARS functionality will be erratic. For example, it might cause the client to go from 11 Mbps directly to 1 Mbps or even disconnect entirely.

While monitoring connectivity to the access point from different distances, also make a point to block the wireless LAN client and access point with items in the environment such as metal blinds, fire doors, concrete walls, etc., to see the effects on the wireless link and throughput. Starting a large file transfer while the laptop is near the access point, walk away from the access point and purposefully interfere with the connection as described above. Notice and record the effects.

Notice that while the FTP session is active, moving away from the access point will show a smoother transition between coverage zones. This is due to the sampling of more frames at the client side of the connection. More samples allow the client to make a better transition between connection speeds.

Process

1. **Configure the network**
   a. Install and configure FTP server software on desktop computer
   b. Install and configure FTP client software on laptop computer
   c. Install and configure throughput-measuring software on laptop computer
   d. Configure all hosts for a flat IP subnet

Copyright © 2003, Planet3 Wireless, Inc.

2. **Configure the Access Point**
    a. Channel 1
    b. SSID=101
    c. 1 mW output power
    d. No WEP
    e. Open System Authentication
3. **Configure the wireless client**
    a. Install and configure drivers
    b. Install and configure wireless LAN utility software
    c. 1 mW output power
    d. SSID=101
    e. No WEP
4. **Testing the link**
    a. Using the signal strength meter and other wireless LAN utilities provided by the manufacturer, determine the RF coverage area around the access point focusing particularly on signal strength, signal-to-noise ratio, and link speed
    b. Determine signal degradation caused by items in the general area around the access point such as concrete walls, metal-mesh windows, metal blinds, etc.
    c. Vary the output power of the access point and the client to show the range of signal at each power level. Keep the power on the access point and client the same as the power levels are increased throughout the exercise.
5. **File transfer**
    a. Start the file transfer from the laptop computer to the desktop computer
    b. Monitor throughput while moving toward and away from the access point
    c. Monitor throughput while putting interfering obstacles between the wireless LAN client and the access point
    d. Verify that the FTP session is not disrupted by the functionality of ARS

Troubleshooting

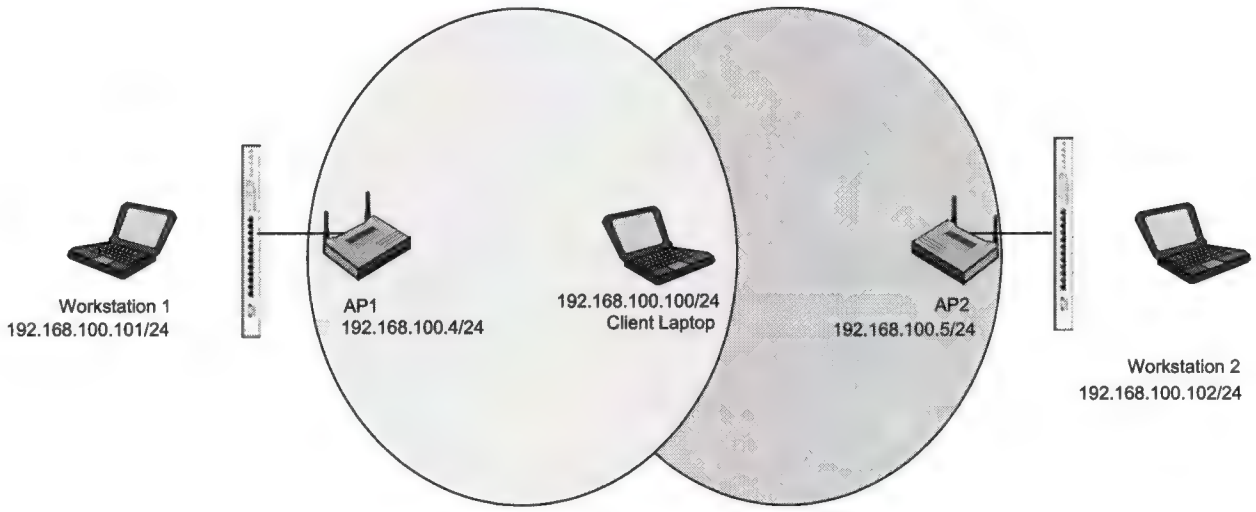
1. Verify WEP & SSID settings are the same on laptop and desktop computers
2. Verify drivers are properly loaded on the wireless LAN client
3. Verify the wireless LAN client is configured in "Infrastructure" mode
4. Verify the radio is turned on in the wireless LAN client

Copyright © 2003, Planet3 Wireless, Inc.

5. Verify username and password on the FTP server are correctly matched with the FTP client
6. Verify connectivity between devices using PING

Copyright © 2003, Planet3 Wireless, Inc.

Lab 5: Rudimentary Security Features



Objective

In this lab exercise, wireless LAN client roaming between access points without losing connectivity is demonstrated. Additionally, the use of SSIDs, MAC filters, and WEP in order to prevent connectivity between a wireless LAN client and the access points are shown.

Hardware/Software required

- 2 Access Points
- 1 Laptop Computer
- 1 wireless LAN PC Card

Copyright © 2003, Planet3 Wireless, Inc.

Summary

This lab exercise will demonstrate roaming between access points by initially configuring both access points and the wireless LAN client with like settings. To verify roaming, installation and configuration of both access points will be done. Having the power output on each access point set to its lowest setting (usually 1mW), creates two cells that have only minimal overlap (if any). Next, as the wireless LAN client moves back and forth between each cell, roaming, association, and disassociation functions occur on the wireless LAN client.

Note: If access points without variable output power settings are used, it may be necessary to turn off one of the access points in order to force the wireless LAN client to roam. Additionally, if this lab is performed in a relatively small space, it may be necessary to turn off one of the access points in order to force roaming regardless of output power settings on the clients and access points.

The next step is to block association to each of the access points using a variety of filtering methods.

- The first, and most rudimentary, method of blocking association is use of the **SSID**, or network name. Changing the SSID of one of the access points will prevent the wireless LAN client from being able to associate to that access point.

- The second method of filtering is the **MAC filter**. The MAC filter on one of the access points will be configured to demonstrate that association can be blocked using this type of filtering.

- The third, and last, simple method of filtering is use of **WEP keys** with shared key authentication. An access point will be configured in shared key authentication mode using a 64-bit (also called 40-bit) WEP key to prevent frames arriving at the access point from being forwarded.

None of these methods are considered secure due to the fact that they only prevent casual eavesdropping on the wireless LAN. However, they do serve as rudimentary security measures and should be used as the most basic forms of wireless LAN security.

Process

1. **Configure the network**
   a. Configure all devices on a flat IP subnet
2. **Configure the Access Points**
   a. Channels 1 & 11
   b. SSID=101
   c. 1 mW output power
   d. No WEP

Copyright © 2003, Planet3 Wireless, Inc.

e. Open System Authentication

3. **Configure wireless LAN client**
   a. SSID=101
   b. No WEP
4. **Verify seamless roaming between access points**
   a. Verify that the wireless LAN client can roam between access points
   b. Verify Layer 2 connectivity by viewing each access point's association table
   c. Verify Layer 3 connectivity by using PING utility
5. **Change the SSID**
   a. Change the SSID on Access Point #1 to 102
   b. Verify that the wireless LAN client can no longer associate to Access Point #1
6. **Configure a MAC filter**
   a. Configure a MAC filter on Access Point #2
   b. Verify that the wireless LAN client can no longer associate to Access Point #2
7. **Configure WEP with Shared-Key Authentication**
   a. Change the SSID on Access Point #1 to 101
   b. Verify that the wireless LAN client can now associate to Access Point #1
   c. Configure Shared-Key Authentication with a 40-bit WEP key of "ABCDEFABCD" on Access Point #1
   d. Verify that the wireless LAN client can no longer associate to Access Point #1
   e. Configure Shared-Key Authentication with a 40-bit WEP key of "ABCDEFABCD" on the wireless LAN client
   f. Verify that the wireless LAN client can now associate to Access Point #1

Troubleshooting

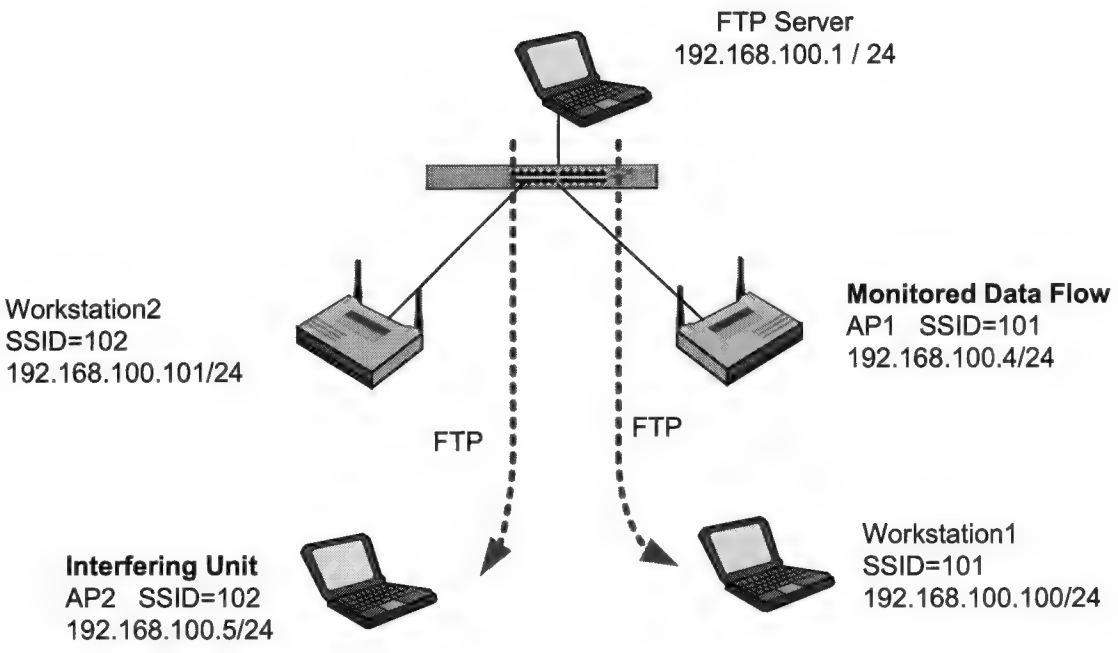
1. Verify WEP & SSID settings are the same on the wireless LAN client and access points
2. Verify drivers are properly loaded on the wireless LAN client
3. Verify wireless LAN client is configured in “Infrastructure” mode
4. Verify radio is turned on in the wireless LAN client and access points
5. Verify Layer 2 connectivity using access points' association tables
6. Verify Layer 3 connectivity using the PING utility
7. Verify no filtering of any kind is configured on the access points

Copyright © 2003, Planet3 Wireless, Inc.

8. Verify that both access points are set to Open System Authentication with no WEP to begin this lab

Copyright © 2003, Planet3 Wireless, Inc.

Lab 6: Co-channel & Adjacent Channel Interference



Objective

In this lab, the effects of co-channel and adjacent channel interference on throughput in a co-located DSSS environment will be demonstrated.

Hardware/Software Required

- 2 Access Points
- 2 Laptop computers
- 2 wireless LAN PC Cards
- 1 Hub
- 1 Desktop Computer
- FTP Server software
- FTP client software
- Throughput-measuring software

Copyright © 2003, Planet3 Wireless, Inc.

Summary

This lab exercise shows the significant negative effects of co-channel and adjacent channel interference. This lends credibility to the suggestion of only co-locating a maximum of two access points. The best co-location performance comes when the two co-located access points have as much channel separation as possible (channel 1 and channel 11 used simultaneously). There are times when moving files simultaneously across the network on various channels produces catastrophic results such as practically no throughput for one of the file transfers. Another method of lessening the effects of co-channel and/or adjacent channel interference is by placing the access points further from each other or decreasing the power output of each (or both techniques simultaneously). These two techniques will significantly improve throughput by decreasing inter-access point interference.

This exercise will also demonstrate that the complete overlapping of channels generally produces more desirable results (better throughput) than does partial overlapping of channels. For example, the results for ch1/ch1 are better than results for ch1/ch3 (severity of degradation depends partially on environment and vendor equipment used).

Process

1. **Configure the network**
   a. Install and configure FTP server software on desktop computer
   b. Install and configure FTP client software on both wireless LAN clients
   c. Install and configure throughput-measuring software on both wireless LAN clients
   d. Configure all hosts for a flat IP subnet
2. **Configure Access Point #1**
   a. Channel 1
   b. SSID=101
   c. No WEP
   d. Open System Authentication
3. **Configure Access Point #2**
   a. Channel 1
   b. SSID=102
   c. No WEP
   d. Open System Authentication

Copyright © 2003, Planet3 Wireless, Inc.

4. **Configure wireless LAN client #1**
    a. Install and configure drivers
    b. Install and configure wireless LAN utility software
    c. SSID=101
    d. No WEP
5. **Configure wireless LAN client #2**
    a. Install and configure drivers
    b. Install and configure wireless LAN utility software
    c. SSID=102
    d. No WEP
6. **File Transfer ch1/ch1 - total overlap**
    a. Begin a file transfer from each of the wireless LAN clients to the FTP Server simultaneously
    b. Monitor throughput on each wireless LAN client and record average throughput for each
7. **File Transfer ch1/ch3 - partial overlap**
    a. Change Access Point #2 to channel 3
    b. Begin a file transfer from each of the wireless LAN clients to the FTP Server simultaneously
    c. Monitor throughput on each wireless LAN client and record average throughput for each
8. **File Transfer ch1/ch6 - non-overlapping**
    a. Change Access Point #2 to channel 6
    b. Begin a file transfer from each of the wireless LAN clients to the FTP Server simultaneously
    c. Monitor throughput on each wireless LAN client and record average throughput for each
9. **File Transfer ch1/ch11 - non-overlapping**
    a. Change Access Point #2 to channel 11
    b. Begin a file transfer from each of the wireless LAN clients to the FTP Server simultaneously
    c. Monitor throughput on each wireless LAN client and record average throughput for each

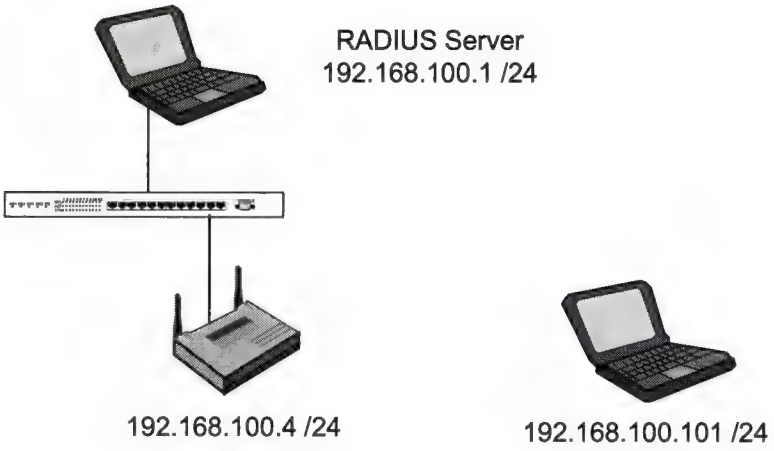
Copyright © 2003, Planet3 Wireless, Inc.

Troubleshooting

1. Verify that wireless LAN client #1 is associating to Access Point #1 by checking Access Point #1's association table. If not associating, check access point#1 and wireless LAN Client #1 settings.
2. Verify that wireless LAN client #2 is associating to Access Point #2 by checking Access Point #2's association table. If not associating, check access point#2 and wireless LAN Client #2 settings.
3. Verify wireless LAN clients can ping the FTP server and have correct FTP login information.
4. Verify drivers are properly loaded on the wireless LAN clients.
5. Verify wireless LAN clients are configured in "Infrastructure" mode.
6. Verify radios are turned on in the wireless LAN clients and access points.
7. Verify no filtering of any kind is configured on the access points.
8. Verify that both access points are set to Open System Authentication with no WEP.

Copyright © 2003, Planet3 Wireless, Inc.

Lab 7: Dynamic WEP keys and mutual authentication using 802.1x/EAP and RADIUS



Objective

In this lab, a popular wireless LAN security solution is shown. This lab is intended to demonstrate the value and use of mutual authentication, dynamic WEP keys, and port-based access control (802.1x).

Hardware/Software Required

- 1 Cisco 1200 series Access Point
- 2 Laptop computers running Windows 2000 Professional with SP3
- 1 Cisco 350 series wireless LAN PC Card
- 1 Hub
- Funk Software Steel-Belted RADIUS Server software v4.0

Copyright © 2003, Planet3 Wireless, Inc.

Summary

This lab exercise demonstrates use of 802.1x and the Extensible Authentication Protocol (EAP) for mutual authentication and dynamic WEP keys for a scalable wireless LAN solution. A wireless LAN card, drivers, firmware, and utility software supporting 802.1x/EAP will be installed on the client computer (laptop). The access point will support 802.1x/EAP, dynamic WEP keys, and RADIUS. The RADIUS server computer and the access point will be connected via a hub.

The RADIUS Server will be installed onto the one laptop for use as the authentication server. A RADIUS server is a centralized authentication server that can generate dynamic encryption keys, verify a user's identity, and assign attributes (privileges) to a user. The access point will forward the user credentials from the client to the RADIUS server for verification after which the access point will allow the client computer onto the network. From that point forward, all frames will use WEP keys that are dynamically generated, regenerated, and distributed from the RADIUS server to the access point and client computer.

Process

1. **Install and configure the RADIUS server**
   a. Install the RADIUS software and appropriately configure for 802.1x/EAP and IP port 1812
   b. Configure the RADIUS server software to take connections from the access point's IP address.
   c. Select the appropriate RADIUS type for proper connection to the access point.
   d. RADIUS key = "key"
   e. Connect the desktop computer to the hub
   f. Configure user*1* in the native RADIUS database with a password of *password*
   g. Configure the RADIUS server to check its native database first
2. **Configure the access point**
   a. Allow encrypted sessions only
   b. Configure for use of EAP and IP port 1812
   c. Channel 1
   d. SSID = 101
   e. RADIUS key = "key"
   f. Enter broadcast WEP key = "ABCDEFABCDEFABCDEFABCDEFAB" into WEP key position #1
3. **Configure the client (laptop)**
   a. Install the client software and choose support for EAP (or LEAP)

Copyright © 2003, Planet3 Wireless, Inc.

b. Configure a profile on the client computer for use of EAP

c. Have EAP manually prompt the user for login credentials (username & password)

d. SSID = 101

4. Prompting for authentication

a. When the client attempts authentication/association with the access point, the client software will automatically prompt the user for the username and password.

5. Enter username and password for RADIUS database

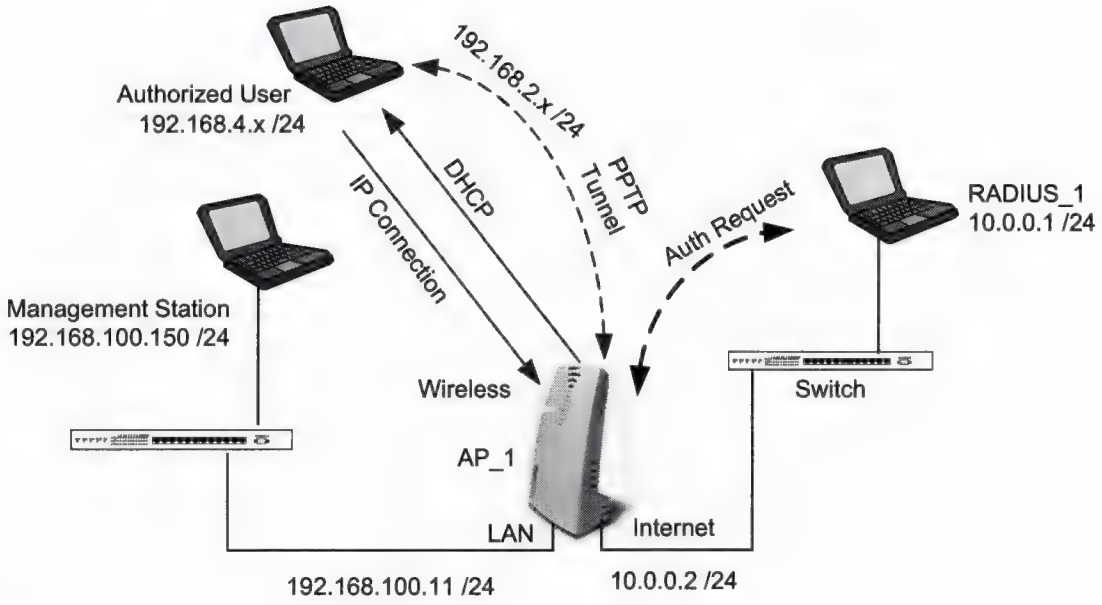
a. Enter the username and password that was entered into the RADIUS server's native database. Verify that the RADIUS server has accepted the connection and verify that the client made a successful connection to the access point by pinging the RADIUS server's IP address.

Troubleshooting

1. Verify that RADIUS server's EAP configuration is correct. This is sometimes done in a text file under the program directory. For example, you might have to verify that the appropriate LEAP section of the EAP.ini file is un-commented out. In order for this type of configuration file to be re-read by the RADIUS application, you must restart the RADIUS service on the server.
2. Verify that the RADIUS server has connected to the appropriate IP address on the server. Sometimes the server will connect to the loopback address (127.0.0.1), which will not work. If this is the case, verify your IP configuration settings on the server. This may also require that you reboot or disable/re-enable an adapter to correct. When RADIUS connects to the manually configured IP address (such as 192.168.1.1), it should work fine.
3. Verify that the access point and the RADIUS share the exact same secret key (also called a password) and IP port number (normally 1812 or 1645). The RADIUS server should have the IP address of the access point, and the access point should have the IP address of the RADIUS server.
4. Verify that you have entered the broadcast WEP key in the first slot (there are 4 slots for entering WEP keys) in the access point's WEP configuration page.

Copyright © 2003, Planet3 Wireless, Inc.

Lab 8: Wireless VPN using PPTP tunnels and RADIUS



Objective

In this lab, a popular wireless LAN security scheme using a virtual private network (VPN) configuration is shown. The wireless LAN client will make a tunneled and encrypted connection with the VPN server (the access point in this case) and will be authenticated locally and via a RADIUS server in different steps of this procedure.

Hardware/Software Required

- 1 Colubris CN1050 Access Point
- 3 Laptop computer running Windows 2000 Professional with SP3
- 1 PC Card
- 2 Hubs
- Funk Software Steel-Belted RADIUS Server software v4.0

Summary

This lab will have the client computer use PPTP VPN client software on the laptop in order to make a dial-up VPN connection with the VPN server (the access point). Current versions of Microsoft Windows support VPN services without any additional third party software. It is suggested to use this built-in VPN software, but third party software may be used provided the Point-to-point Tunneling

Copyright © 2003, Planet3 Wireless, Inc.

Protocol (PPTP) is supported. In the first part of this lab, the VPN server will have its own native user database configured. The client computer (laptop) will dial into the IP address of the access point using an authorized username and password that has been pre-configured on the access point.

In the second part of this lab, the client will again dial into the access point, but the access point will now be configured to pass along authentication (username and password) information to a RADIUS server that has been configured for a username and password. The RADIUS server will verify the username and password from the client computer is valid, and notify the access point to continue building the VPN tunnel. The access point will pass an IP address to the client computer for the client end of the VPN tunnel. Once the tunnel is built, the client computer will be able to ping the RADIUS server proving that the VPN server is now passing traffic upstream from downstream tunnels. Before the VPN tunnel is built, the client will not be able to pass traffic upstream into the wired LAN.

Process

1. **Install and configure the RADIUS server**
   a. Install and configure the RADIUS server software to take connections from the access point's IP address
   b. Select the appropriate RADIUS type for proper connection to the access point (Standard IETF RADIUS)
   c. RADIUS key = "key"
   d. Connect the RADIUS server to the hub
2. **Configure the Management Station**
   a. Set the IP address to the same subnet as the access point's LAN interface
   b. Connect the configuration PC to the hub
   c. Using a web browser, browse to the IP address of the access point's LAN interface
3. **Configure the Access Point (VPN Server)**
   a. The LAN IP address of the VPN Server should be pre-configured by the instructor and labeled on the case of the unit
   b. SSID = 101
   c. Channel = 1
   d. Security mode = PPTP
   e. Authentication mode = local
   f. Configure VPN tunnel IP subnet for 192.168.2.x /24
   g. Configure a user in the VPN server and another (different) user in the native RADIUS database. Give each of these two users a password of "password" – a suggestion for usernames is "user1" and "user2". Configuration of users on the RADIUS server will require that the RADIUS

Copyright © 2003, Planet3 Wireless, Inc.

server return two attributes for these users to the VPN server. These return attributes will be "MPPE-Recv-Key" and "MPPE-Transmit-Key" and are chosen out of a list in the RADIUS server configuration.

4. **Configure the client PC**

   a. Configure the wireless PC card drivers and utilities

   b. Configure the client PC (laptop) for a PPTP dial-up VPN connection to the VPN server using the VPN server's IP address and the username and password that were entered into the VPN Server itself.

5. **Use PPTP to dial the VPN server & verify connectivity**

   a. Attempt a connection between the client PC and the VPN server using the username entered into the VPN server's database

   b. The client PC should establish a tunnel connection to the VPN server

   c. Verify connectivity to the VPN server by opening a console window and typing "winipcfg" (for Windows 95, 98, & ME) or "ipconfig" (for Windows NT, 2000, and XP). You should see an adapter with your 192.168.100.x address and a VPN adapter with an IP address from the tunnel subnet (192.168.2.x)

   d. Disconnect the client PC from the VPN server

6. **Reconfigure Access Point (VPN Server)**

   a. Configure VPN server for "RADIUS profile 1" where the VPN server no longer uses its native database, but rather the RADIUS database.

   b. Configure the VPN server for the RADIUS server's IP address, port 1812, and the RADIUS key = "key"

   c. Configure the WAN interface of the VPN server for an IP address on the same subnet as the upstream RADIUS server.

   d. Verify that the RADIUS server can ping the WAN interface of the VPN server.

7. **Use PPTP to dial the VPN server & verify connectivity**

   a. Attempt a connection between the client PC and the VPN server using the username entered into the RADIUS server's database.

   b. The client PC should establish a tunnel connection to the VPN server

   c. Verify connectivity to the VPN server by opening a console window and typing "winipcfg" (for Windows 95, 98, & ME) or "ipconfig" (for Windows NT, 2000, and XP). You should see an adapter with your 192.168.100.x address and a VPN adapter with an IP address from the tunnel subnet (192.168.2.x)

   d. Disconnect the client PC from the VPN server

Troubleshooting

1. Verify that the RADIUS server and VPN server keys match exactly
2. Verify that the RADIUS server can ping the VPN server
3. Verify that the VPN software on the client is set for PPTP
4. Verify usernames and passwords are entered into the proper places and are spelled correctly in each place
5. Verify that the VPN server has the latest firmware revision

Copyright © 2003, Planet3 Wireless, Inc.

Optimized Network Education

COURSE EVALUATION

Course Title: _____ Course Number: _____

Your Instructor: _____ Course Dates: _____

Location: _____ Your Name (Optional): _____

Your Job Classification (Check One):

__ Field Engineer __ Network Engineer __ Network Administrator

__ Software Engineer __ Help Desk __ Data Base Administrator

__ Independent Consultant __ Technical Instructor __ Manager / Supervisor

__ Other (Please specify: _____)

Please rate this course, the course material, the logistics, and your instructor by indicating your degree of Agreement (⑤) or Disagreement (①) with each of the following statements. A ⑤ is a high score and a ① is a low score.

		① = Disagree				⑤ = Agree
Logistics						
1.	The process of registering for this course was easy.	①	②	③	④	⑤
2.	The classroom temperature was comfortable	①	②	③	④	⑤
3.	The classroom was the right size and layout for this class	①	②	③	④	⑤
Course Organization And Material						
4.	The course manual was easy to understand and use	①	②	③	④	⑤
5.	The course content was well organized	①	②	③	④	⑤
6.	The course manual will serve as a reference for me in the future	①	②	③	④	⑤
7.	The scope and depth of the material was at the right level for the class	①	②	③	④	⑤
8.	The "Follow Along" demonstration exercises were useful	①	②	③	④	⑤
9.	The "Hands On", independent exercises were useful	①	②	③	④	⑤
10.	I had sufficient time to practice the hands-on exercises	①	②	③	④	⑤
Instructor Effectiveness						
11.	The instructor seemed knowledgeable in the subject	①	②	③	④	⑤
12.	The instructor's explanations were clear	①	②	③	④	⑤
13.	The instructor responded to questions thoroughly	①	②	③	④	⑤
14.	The methods, manners, and approaches used by the instructor were effective	①	②	③	④	⑤
15.	The instructor made good use of time	①	②	③	④	⑤
16.	The instructor added technical value to the material	①	②	③	④	⑤
17.	The instructor kept to the topic in an orderly manner	①	②	③	④	⑤
Overall Assessment						
18.	This was an excellent class and I got a lot out of it	①	②	③	④	⑤
19.	This training seminar exceeded my expectations	①	②	③	④	⑤
20.	My personal level of expertise increased dramatically from this class	①	②	③	④	⑤

CONTINUED ON THE BACK...

Please help us understand who you are and what you do so that we may better understand our marketplace. Select one response from each group below.

21. **How often do you use a protocol analyzer?**
- ❑ Never
- ❑ Occasionally
- ❑ Regularly
- ❑ Every Day

22. **How long have you been using a protocol analyzer?**
- ❑ This class is the first time I've ever actually used one
- ❑ I have experimented with my analyzer at work but only recently
- ❑ I have been using an analyzer for about six months
- ❑ I have been using analyzers for over a year
- ❑ I have been using analyzers for years

23. **How much do you know about protocol internal engineering?**
- ❑ I know very little about networking in general
- ❑ I know about the installation and configuration of networks but less about protocols
- ❑ I know about certain protocols but less about installation and configuration
- ❑ I am reasonably experienced in at least one major protocol family
- ❑ I am considered a protocol analysis expert

What industry certifications do you currently hold (CNX, MCSE, CCIE, A+, etc.) _____

YOUR COMMENTS:

Please take a moment and write a short evaluation of your training experience and include any suggestions that you have for improvement. This is the most important portion of the Course Evaluation process so you are greatly encouraged to respond!

If you have a positive experience and comment can we quote you?

To the Press? Yes _____ No _____
In Print? Yes _____ No _____
On our Web Site? Yes _____ No _____
Signature Approval: _____

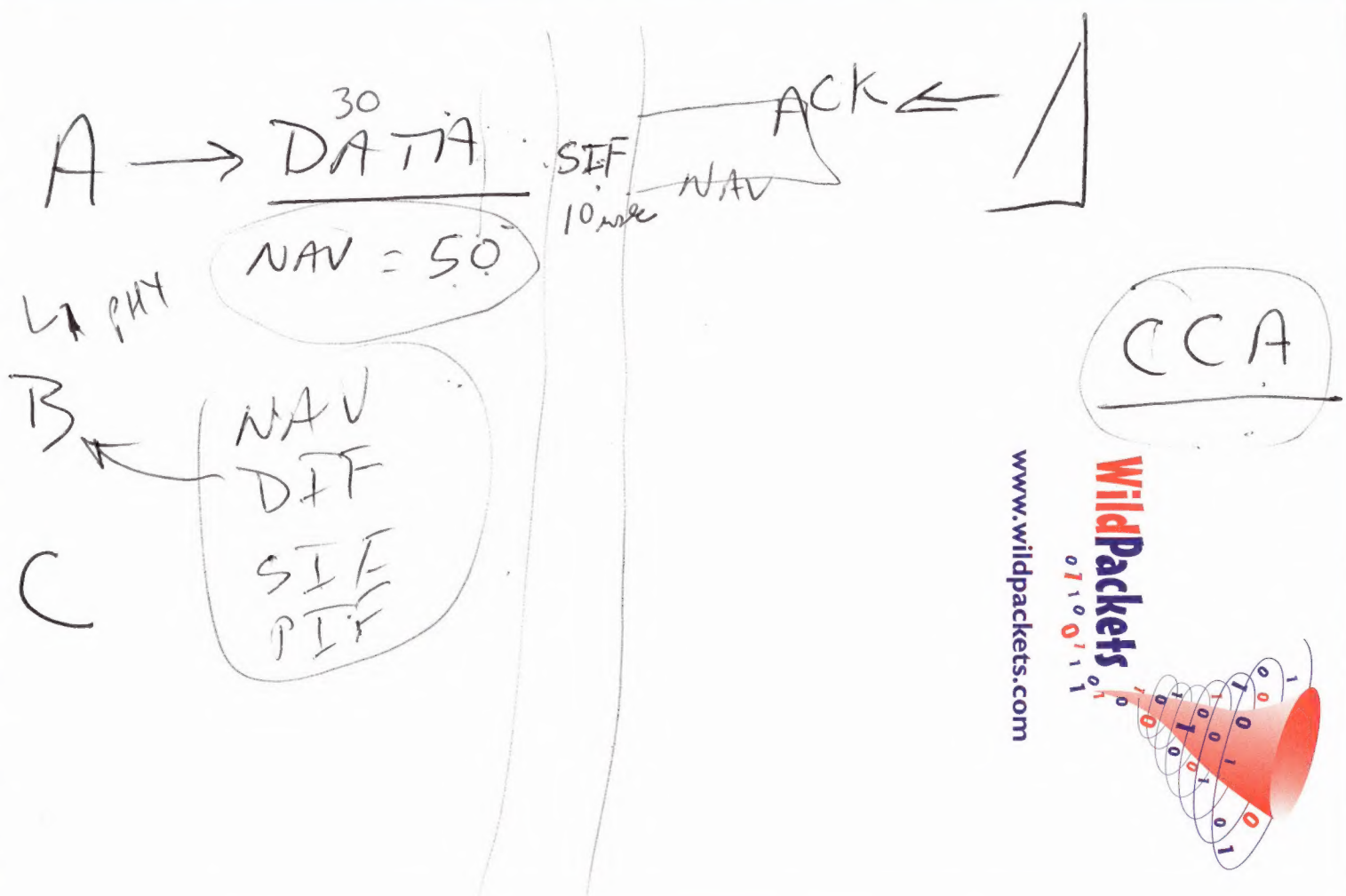
Are there other people or organizations within your company who might be interested in taking a WildPackets Academy **training course?** ❑

Is there someone we may contact within your company regarding providing WildPackets Professional Services Support such as **on-site or remote consulting?** ❑

Contact Name: _____ Contact Phone: _____

Contact Email/Address: _____

Thank You for attending this Optimized Network Education training seminar!



WildPackets
www.wildpackets.com